HIGHER ALGEBRA I (MATH 570)
COURSE NOTES
FALL 2018
VERSION: December 22, 2018

EYAL Z. GOREN,
MCGILL UNIVERSITY

Contents

Part 1. Categories and Functors I

The good news is that categories are all around us. Without ever mentioning it, we have systematically used categories in previous courses. When restricting our attention to k-vector spaces and k-linear maps, we have been working in the category **kVSp** of k-vector spaces. When considering groups and group homomorphisms, we were working in the category **Gps** of Groups. Even more basic is the category **Sets** of sets with functions between sets. Topological spaces form a category **Top** with maps being continuous maps; when we consider pairs (X,x) where X is a topological space and $x \in X$ is a point we would like to consider only maps $f\colon (X,x) \to (Y,y)$, meaning continuous maps $f\colon X \to Y$ such that $f(x) = y$. This defines the category $\star$**Top** of pointed topological spaces.

The use of functors, on the other hand, was rather restricted. Functors are a tool to pass from one category to another and usually require more sophisticated mathematics, to go beyond trivial constructions. Perhaps the prettiest example is associated to a topological pointed space (X,x) its fundamental group $\pi(X,x)$. This provides a functor $\star$**Top** $\to$ **Gps**. Another example that is important is the duality functor **kVSp** $\to$ **kVSp** sending a vector space V to its dual $V^* = \mathrm{Hom}_k(V,k)$ and a linear map $T\colon V \to W$ to its dual $T^*\colon W^* \to V^*$, $(T^*f)(v) := f(Tv)$..

1. First definitions

1.1. **Categories.** A **category C** consists of several pieces of data:

- A collection of **objects** Ob **C**.
- For any two objects A, B a set of **morphisms** $\mathrm{Mor}(A,B)$ (or $\mathrm{Mor}_{\mathbf{C}}(A,B)$, if we need to be more precise).
- For any three objects A,B,C, a function $\mathrm{Mor}(A,B) \times \mathrm{Mor}(B,C) \to \mathrm{Mor}(A,C)$ that we denote $(f,g) \mapsto g \circ f$.
- For every object A, a morphism $1_A \in \mathrm{Mor}(A,A) =: \mathrm{End}(A)$.

These are required to satisfy:

$$h \circ (g \circ f) = (h \circ g) \circ f, \qquad f \circ 1_A = f, \qquad 1_B \circ f = f,$$

for $f \in \mathrm{Mor}(A,B), g \in \mathrm{Mor}(B,C), h \in \mathrm{Mor}(C,D)$.

It is easy to check that 1_A is unique. A morphism $f \in \mathrm{Mor}(A,B)$ is called an **isomorphism** if there is a morphism $g \in \mathrm{Mor}(B,A)$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. If $g' \in \mathrm{Mor}(B,A)$ is another morphism satisfying $f \circ g' = 1_B$ then $g = g'$.

Examples of categories are a plenty. We have already seen: **Sets**, **Gps**, **kVSp**, **Top**, $\star$ **Top**. Here are some additional examples.

(1) The category of rings **Rings** consists of rings (always associative with 1, but non-necessarily commutative) and ring homomorphisms (always taking 1 to 1).

(2) The categories ${}_{\mathbf{R}}\mathbf{Mod}$ and $\mathbf{Mod}_{\mathbf{R}}$. Let R be a ring and denote ${}_{\mathbf{R}}\mathbf{Mod}$ (respectively, $\mathbf{Mod}_{\mathbf{R}}$) the category of left R-modules (resp., right R-modules). Morphisms are homomorphism of modules. That is, morphisms are functions,

$$f\colon M_1 \to M_2,$$

that satisfy

$$f(x+y) = f(x) + f(y), \quad f(rx) = rf(x), \quad \forall x,y \in M_1, r \in R.$$

(For right R-modules we require $f(xr) = f(x)r, \forall x \in M_1, r \in R$.) To simplify notation we define

$$\mathrm{Hom}_R(A, B) := \mathrm{Mor}_{\mathbf{_RMod}}(A, B).$$

Let **AbGps** be the category whose objects are abelian groups and whose morphisms are group homomorphisms. Then $\mathbf{AbGps} = {}_{\mathbb{Z}}\mathbf{Mod} = \mathbf{Mod}_{\mathbb{Z}}$. Similarly, for k a field, $\mathbf{kVSp} = {}_{\mathbf{k}}\mathbf{Mod}$. To give an object in the category ${}_{\mathbf{k[x]}}\mathbf{Mod}$ is to give a k-vector space M and a k-linear map $T\colon M \to M$ recording the action of x. That is, $xm = T(m)$ defines T and, more generally, for any polynomial $f(x) \in k[x]$, $f(x)m = f(T)(m)$.

(3) The category ${}_{\mathbf{R}}\mathbf{Mod}_{\mathbf{S}}$. Let R and S be rings. An **bimodule** M is an abelian group M that is at the same time a left R-module and a right S-module and such that for all $m \in M$, $r \in R, s \in S$, we have

$$(rm)s = r(ms).$$

Morphisms are homomorphisms of groups $f\colon M_1 \to M_2$ that satisfy

$$f(r \cdot x \cdot s) = r \cdot f(x) \cdot s.$$

For example, let k be a field and let a, b, be positive integers, $R = M_a(k)$, $S = M_b(k)$, the rings of $a \times a$ and $b \times b$ matrices with entries in k. Then the $a \times b$ matrices $M_{a,b}(k)$ with matrix addition are an object of ${}_{\mathbf{R}}\mathbf{Mod}_{\mathbf{S}}$ under matrix multiplication. Another simple observation is that always $R \in {}_{\mathbf{R}}\mathbf{Mod}_{\mathbf{R}}$ and ${}_{\mathbf{R}}\mathbf{Mod} = {}_{\mathbf{R}}\mathbf{Mod}_{\mathbb{Z}}$, $\mathbf{Mod}_{\mathbf{R}} = {}_{\mathbb{Z}}\mathbf{Mod}_{\mathbf{R}}$. The category ${}_{\mathbf{k[x]}}\mathbf{Mod}_{\mathbf{k[x]}}$ is interesting. To give a bimodule in this category is equivalent to giving a k-vector space V with two commuting linear maps $S, T\colon V \to V$ (indeed, one lets $T(v) = xv$ and $S(v) = vx$.

Notation. To simplify notation, instead of saying that A is a left R-module, we shall sometimes say that ${}_RA$ is a module; similarly, we say that A_R is a module and mean that A is a right R-module. Also, we will say that ${}_RA_S$ is a bimodule to mean that it is an object of ${}_{\mathbf{R}}\mathbf{Mod}_{\mathbf{S}}$. Thus, we will often use the symbols

$${}_RA, \quad A_R, \quad {}_RA_S.$$

(4) It is important to note that although in many examples of a categories morphisms are functions, this need not be the case in general. For example: let G be a group and define a category $*_{\mathbf{G}}$ with a single object $*$ and with $\mathrm{Mor}(*, *) = G$, where the composition law is just multiplication in the group:

$$\mathrm{Mor}(*, *) \times \mathrm{Mor}(*, *) \longrightarrow \mathrm{Mor}(*, *), \qquad (f, g) \mapsto fg.$$

1.2. **Functors.** Functors are an intelligent way to pass from one category to another. Given objects in a category $\mathbf{C}$ a functor F associates to them objects in a category $\mathbf{D}$. For this to be interesting we should allow relations between two objects in $\mathbf{C}$ to become relations between the objects associated to them in $\mathbf{D}$. To be a precise:

Let $\mathbf{C}, \mathbf{D}$ be categories. A **covariant** (respectively, **contravariant**) **functor**

$$F\colon \mathbf{C} \to \mathbf{D},$$

associates to every object A of $\mathbf{C}$ and object $F(A)$ (or simply FA) of $\mathbf{D}$ and to any morphism $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$ a morphism $F(f)$ (or simply Ff) in $\mathrm{Mor}_{\mathbf{D}}(FA, FB)$ (resp., in $\mathrm{Mor}(FB, FA)$), such that:

$$F1_A = 1_{FA}, \qquad F(g \circ f) = Fg \circ Ff, \qquad (\text{resp., } F(g \circ f) = Ff \circ Fg).$$

We say that

- F is **faithful** if for any objects A, B of $\mathbf{C}$ and morphisms $f, g \in \mathrm{Mor}(A, B)$, $Ff = Fg$ implies $f = g$;
- F is **full** if any $h \in \mathrm{Mor}_{\mathbf{D}}(FA, FB)$ is equal to Ff for some $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$ (and with obvious modifications for contravariant functors).

- Also, if F is full and faithful we say it is **fully faithful**.

Here are some examples:

(1) **Forgetful functors**. Those can be defined for any category whose objects are sets (possibly with additional structure) and whose morphisms are (possibly restricted) functions of sets. To illustrate, define

$$\Phi\colon \textbf{Gps} \to \textbf{Sets},$$

by

$$\Phi(A) = A, \quad \Phi(f) = f.$$

Namely, Φ "forgets" that A is a group and f is a homomorphism of groups and only "remembers" that A is a set and f is a function between sets. This is a covariant functor, which is faithful but not full.

(2) **Abelianization**. Consider the functor **Gps** → **AbGps**, given on objects by

$$G \mapsto G^{ab} := G/G',$$

where G' is the commutator group. Given a group homomorphism $f\colon G \to H$ we get a well defined homomorphism,

$$G^{ab} \to H^{ab}, \quad gG' \mapsto f(g)H',$$

that we denote f^{ab}. This is a covariant functor that is neither full nor faithful.

(3) **Sheaves.** Let X be a topological space and consider the collection of open sets of X as the objects of a category $\mathcal{T}_{\mathbf{X}}$, whose morphisms are

$$\mathrm{Mor}(U,V) = \begin{cases} \iota_{U,V}, & U \subseteq V, \\ \emptyset, & U \nsubseteq V. \end{cases}$$

A **pre-sheaf** of abelian groups is a contravariant functor:

$$\mathcal{O}\colon \mathcal{T}_{\mathbf{X}} \to \textbf{AbGps},$$

such that $\mathcal{O}(\emptyset) = 0$ (the abelian group with one element 0). Explicitly, for every open set U we are given an abelian group $\mathcal{O}(U)$, and for every inclusion $U \subseteq V$, a group homomorphism, that we denote $res_{V,U}$ and call restriction, from $\mathcal{O}(V) \to \mathcal{O}(U)$. The restriction homomorphisms respect compositions and $res_{V,V} = 1_{\mathcal{O}(V)}$. We can obviously replace in this definition **AbGps** by **Sets**, **Gps**, **Rings**, but the most common choices, besides abelian groups, are either k-vector spaces (for some fixed field k, such as $\mathbb{R}$ or $\mathbb{C}$) and commutative rings. Sheaves are central to modern geometry and topology.

As a specific example, let $X = \mathbb{R}^n$ and let $\mathcal{O}(U)$ denote the ring $C(U)$ of continuous functions $f\colon U \to \mathbb{R}$. We can also take $\mathcal{O}(U) = C^\infty(U)$, the infinitely differentiable functions $f\colon U \to \mathbb{R}$. Many variants exist.

A **sheaf** is a pre-sheaf that has the properties that its values are determined by local data and that local data glues. To be precise, we require: (i) if $U = \cup U_\alpha$ is a a union of open sets and $f \in \mathcal{O}(U)$ is such that $res_{U,U_\alpha} f = 0$ for all α then $f = 0$; (ii) Given $f_\alpha \in \mathcal{O}(U_\alpha)$ such that for all α, β we have $res_{U_\alpha, U_{\alpha\cap\beta}} f_\alpha = res_{U_\beta, U_{\alpha\cap\beta}} f_\beta$ then there exists $f \in \mathcal{O}(U)$ such that $res_{U,U_\alpha} = f_\alpha$ for all α.

(4) Let G, H be groups. A covariant functor $F : *_{\mathbf{G}} \to *_{\mathbf{H}}$ amounts to a group homomorhism $G \to H$.

(5) Let G be a group and let k be a field. Define the **group ring** $k[G]$ to be the ring whose elements are formal sums

$$\sum_{g \in G} a_g g, \quad a_g \in k, \text{ almost all } a_g = 0,$$

with addition

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g + b_g)g$$

and multiplication

$$(\sum_{g\in G} a_g g)(\sum_{g\in G} b_g g) = \sum_{g\in G}(\sum_{h\in G} a_h b_{h^{-1}g})g.$$

Occasionally, when it helps clarifying the argument, we also denote an element of $k[G]$ as

$$\sum_{g\in G} a_g[g].$$

It is not hard (except on my fingers typing this text) to verify that this is a ring which is non-commutative if G is not commutative. Moreover, there is a obvious covariant functor **Gps** → **Rings** taking G to $k[G]$ and $f : G \to H$ to $f : k[G] \to k[H]$ given by

$$f(\sum_g a_g g) = \sum_g a_g f(g).$$

(6) **Hom.** Let R be a ring and fix an object $A \in {}_{\mathbf{R}}\mathbf{Mod}$ (the variant $A \in \mathbf{Mod}_{\mathbf{R}}$ is left to the reader). We get then two functors:

$$\mathrm{Hom}_R(A, -) : {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{AbGps}, \qquad \text{(covariant)},$$

and

$$\mathrm{Hom}_R(-, A) : {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{AbGps}, \qquad \text{(contravariant)}.$$

In each case the group law is that $f + g$ is the homomorphism of modules given by $(f + g)(x) = f(x) + g(x)$. An important observation is that if A is an object of ${}_{\mathbf{R}}\mathbf{Mod}_{\mathbf{S}}$ then in fact

$$\mathrm{Hom}_R(A, -) : {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{S}}\mathbf{Mod}, \qquad \text{(covariant)},$$

and

$$\mathrm{Hom}_R(-, A) : {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{Mod}_{\mathbf{S}}, \qquad \text{(contravariant)}.$$

In the first case we define $(sf)(a) = f(as)$ (a key point is that $(s(tf))(a) = (tf)(as) = f((as)t) = f(a(st)) = ((st)f)(a)$ and therefore $s(tf) = (st)f$, which is needed to make $\mathrm{Hom}_R(A, B)$ into a left S-module). In the second case define $(fs)(b) = f(b) \cdot s$ (and one finds $f(st) = (fs)t$). Typically, these functors are neither full nor faithful.

Remark 1.2.1. When R is a commutative ring and R-module ${}_RA$ is automatically an R-bimodule where we define right multiplication by $a \cdot r := ra$, $a \in A, r \in R$. Note that the bimodule condition $r \cdot (a \cdot s) = (r \cdot a) \cdot s$ holds because R is commutative. Thus, when R is commutative, the functors $\mathrm{Hom}_R(A, -), \mathrm{Hom}_R(-, A)$ always take value in ${}_{\mathbf{R}}\mathbf{Mod}$ and just in **AbGps**.

2. Morphisms of functors

2.1. **Natural equivalence.** If this is not abstract enough, here comes another layer of abstraction. Let F, G, be functors $\mathbf{C} \to \mathbf{D}$ of the same variance. A **morphism of functors** (also called a **natural transformation**)

$$\varphi\colon F \to G,$$

is a collection of morphisms $\varphi_A \colon FA \to GA$ for every object A of $\mathbf{C}$ [1] that are compatible in the following sense: for any $f\colon A \to B$ the following diagram commutes:

$$\begin{tikzcd}
FA \arrow[r, "\varphi_A"] \arrow[d, "Ff"'] & GA \arrow[d, "Gf"] \\
FB \arrow[r, "\varphi_B"] & GB.
\end{tikzcd}$$

(The diagram for contravariant functors is similar – the vertical arrows would go up, though.) If for every A the morphism φ_A is an isomorphism then we say that F and G are **isomorphic** (or **naturally equivalent**).

Example 2.1.1. Let R be a ring and let ${}_RM$ be a module. We have an isomorphism

$$\varphi_M \colon \mathrm{Hom}_R(R, M) \cong M. \qquad \varphi_M(\alpha) = \alpha(1).$$

The collection of maps $\{\varphi_M\}$ provides an isomorphism of functors between the functor

$$\mathrm{Hom}_R(R, -)\colon {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{R}}\mathbf{Mod}$$

and the **identity functor**

$$\mathbb{1}\colon {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{R}}\mathbf{Mod}, \qquad \mathbb{1}(M) = M,\ \ \mathbb{1}(f) = f.$$

2.2. **Adjoint functors.** Let $F\colon \mathbf{C} \to \mathbf{D}$ and $G\colon \mathbf{D} \to \mathbf{C}$ be functors of the same variance. We say that $(F, G)$is an **adjoint pair** of functors[2], or that F is **left-adjoint** to G, or that G is **right-adjoint** to F (and this is also denoted $F \dashv G$) if for any objects A of $\mathbf{C}$ and B of $\mathbf{D}$ we have isomorphisms

$$\mathrm{Mor}_{\mathbf{D}}(FA, B) \xrightarrow[\cong]{\varphi_{A,B}} \mathrm{Mor}_{\mathbf{C}}(A, GB),$$

such that for every $f \in \mathrm{Mor}(A, A'), g \in \mathrm{Mor}(B, B')$ the following diagrams commute. (We are writing them for the covariant case; the contravariant case is very similar.)

$$\begin{tikzcd}
\mathrm{Mor}_{\mathbf{D}}(FA, B) \arrow[r, "\varphi_{A,B}"] & \mathrm{Mor}_{\mathbf{C}}(A, GB) \\
\mathrm{Mor}_{\mathbf{D}}(FA', B) \arrow[r, "\varphi_{A',B}"] \arrow[u, "(-)\circ Ff"] & \mathrm{Mor}_{\mathbf{C}}(A', GB), \arrow[u, "(-)\circ f"']
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathrm{Mor}_{\mathbf{D}}(FA, B) \arrow[r, "\varphi_{A,B}"] \arrow[d, "g\circ(-)"'] & \mathrm{Mor}_{\mathbf{C}}(A, GB) \arrow[d, "Gg\circ(-)"] \\
\mathrm{Mor}_{\mathbf{D}}(FA, B') \arrow[r, "\varphi_{A,B'}"] & \mathrm{Mor}_{\mathbf{C}}(A, GB').
\end{tikzcd}$$

Taking the case $B = FA_1$, we find isomorphisms

$$\mathrm{Mor}_{\mathbf{D}}(FA, FA_1) \xrightarrow[\cong]{\varphi} \mathrm{Mor}_{\mathbf{C}}(A, GFA_1)\ ,$$

and, in particular, for $A_1 = A$ we get a morphism

$$\varphi(1_{FA})\colon A \to GFA,$$

called the **unit** of the adjoint pair. So, in some *weak sense*, we think of G as a left-inverse to F.

A simple example is the following. Let $Inc\colon \mathbf{AbGps} \to \mathbf{Gps}$ be the inclusion functor, $Inc(G) = G, Inc(f) = f$. Let $ab\colon \mathbf{Gps} \to \mathbf{AbGps}$ be the abelianization functor discussed before. Then the pair (ab, Inc) is an adjoint pair. That is, we have natural isomorphisms,

$$\mathrm{Hom}(G^{ab}, A) \cong \mathrm{Hom}(G, A),$$

[1] Here, and often later, we abuse notation and write $\varphi_A \colon FA \to GA$ instead of $\varphi_A \in \mathrm{Mor}(FA, GA)$. It is an abuse of notation, because φ_A need not be a function as the arrow suggests – we don't assume that $\mathrm{Mor}(FA, GA)$ consists of functions.

[2] Rotman in "Advanced Modern Algebra" unfortunately denotes this by (G, F).

for any group G and any abelian group A. The unit is the canonical map $G \to G^{ab}$.

It is usually a very fruitful question to ask whether a functor F has an adjoint; we shall see later this always implies good properties for F. In general, a functor need not have an adjoint (left, or right) and it is possible that it has both left and right adjoints, but they are different.

2.3. **The adjoint to the forgetful functor.** Consider the forgetful functor

$$\Phi\colon \mathbf{Gps} \to \mathbf{Sets}.$$

We wish to construct a functor

$$F\colon \mathbf{Sets} \to \mathbf{Gps}$$

such that (F, Φ) are an adjoint pair. That means that we want natural isomorphisms

$$\mathrm{Hom}_{\mathbf{Gps}}(F(S), G) \cong \mathrm{Mor}_{\mathbf{Sets}}(S, \Phi(G)),$$

where, recall, $\Phi(G)$ is the just the underlying set of G. The group $F(S)$ is called the **free group** on the alphabet S and F the **free construction** functor. Before constructing $F(S)$, we remark that for many categories besides **Gps** such constructions are possible. For example $\mathbf{AbGps}, \mathbf{kVSp}, {}_{\mathbf{R}}\mathbf{Mod}, \mathbf{Top}$, and so on.

We first consider **words** in the alphabet S. These are strings (the empty string is allowed, even welcomed!) of the form

$$w_1^{\epsilon_1} \cdots w_s^{\epsilon_s}, \qquad w_i \in S, \epsilon_i = \pm 1.$$

We put an equivalence relation on words by decreeing

$$w_1^{\epsilon_1} \cdots w_s^{\epsilon_s} \sim w_1^{\epsilon_1} \cdots w_i^{\epsilon_i} t^{\epsilon} t^{-\epsilon} w_{i+1}^{\epsilon_{i+1}} \cdots w_s^{\epsilon_s},$$

for any $t \in S, \epsilon = \pm 1, 0 \leq i \leq t$. For example, if $S = \{x, y\}$ the following are equivalent words:

$$xxy, yy^{-1}xxy^{-1}yy, xxyxx^{-1}, xyy^{-1}xx^{-1}yy^{-1}xy,$$

etc. We will often be sensible and write xxy as x^2y, etc., as shorthand. We denote the equivalence class of $w_1^{\epsilon_1} \cdots w_s^{\epsilon_s}$ by $[w_1^{\epsilon_1} \cdots w_s^{\epsilon_s}]$ and the set of equivalence classes by $F(S)$. The set $F(S)$ has a natural structure of a group under the composition rule

$$[w_1^{\epsilon_1} \cdots w_s^{\epsilon_s}][z_1^{\delta_1} \cdots z_t^{\delta_t}] = [w_1^{\epsilon_1} \cdots w_s^{\epsilon_s} z_1^{\delta_1} \cdots z_t^{\delta_t}]$$

(well-defined!), identity being the empty word, and inverse given by

$$[w_1^{\epsilon_1} \cdots w_s^{\epsilon_s}]^{-1} = [w_s^{-\epsilon_s} \cdots w_1^{-\epsilon_1}].$$

Proposition 2.3.1. *Let S be a set and G be a group. Let*

$$f\colon S \to G$$

be a function. There is a unique homomorphism that we likewise denote f,

$$f\colon F(S) \to G,$$

such that $f([s]) = f(s), \forall s \in S$.

Proof. The important point is to check that letting

$$f([w_1^{\epsilon_1} \cdots w_s^{\epsilon_s}]) = f(w_1)^{\epsilon_1} \cdot f(w_2)^{\epsilon_2} \cdots f(w_s)^{\epsilon_s},$$

is a well defined function $F(S) \to G$. This amounts to checking that if we calculate f using $w_1^{\epsilon_1} \cdots w_i^{\epsilon_i} t^{\epsilon} t^{-\epsilon} w_{i+1}^{\epsilon_{i+1}} \cdots w_s^{\epsilon_s}$ we will get the same value. This is clear. The fact that f is a homomorphism follows immediately from the definition. □

Corollary 2.3.2. *If S has at least two elements $F(S)$ is a non-commutative infinite group.*

Proof. For every $n \geq 2$, S_n is generated by (12) and $(123\cdots n)$. Choose two distinct elements s_1, s_2 in S and define a homomorphism $f\colon F(S) \to S_n$ by $f(s_1) = (12), f(s_2) = (123\cdots n)$ and for any other $s \in S$, $f(s) = 1$. As these are surjective homomorphisms for every $n \geq 2$ and $|S_n| = n!$ it follows that $F(S)$ is non-commutative and infinite. □

In fact, already $F(S)$ for $S = \{x, y\}$ is "enormous". One can prove that for any finitely generated group G, and, in particular, for any finite group G, there is a subgroup $H < F(S)$ of finite index and a surjective homomorphism $f\colon H \to G$.

Getting back to our business: showing now that (F, Φ) is an adjoint pair, namely that we have compatible isomorphisms

$$\varphi_{S,G}\colon \mathrm{Hom}_{\mathbf{Gps}}(F(S), G) \to \mathrm{Mor}_{\mathbf{Sets}}(S, G),$$

is now an easy matter. To a homomorphism $f\colon F(S) \to G$ assign the function, still denoted f,

$$S \to G, \quad s \mapsto f([s]).$$

To a function $f\colon S \to G$ assign the group homomorphism, still denoted f,

$$f\colon F(S) \to G$$

as in the proposition. Namely, $f([w_1^{\epsilon_1}\cdots w_s^{\epsilon_s}]) = f(w_1)^{\epsilon_1}\cdot f(w_2)^{\epsilon_2}\cdots f(w_s)^{\epsilon_s}$.

A question that we would like to ask is the following: Let R, S be rings and let A be a bimodule in ${}_{\mathbf{S}}\mathbf{Mod}_{\mathbf{R}}$. We have a covariant functor

$$\mathrm{Hom}_S(A, -)\colon {}_{\mathbf{S}}\mathbf{Mod} \to {}_{\mathbf{R}}\mathbf{Mod}.$$

Does this functor have an adjoint?? We are going to build for it a left-adjoint by means of tensor products.

Part 2. Modules I

Let R be a ring and let A_R and ${}_RB$ be modules. An R**-biadditive map** $A \times B \to H$, where H is an abelian group, written additively, is a function

$$f\colon A \times B \to H$$

that satisfies:

(1) $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$;
(2) $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$;
(3) $f(ar, b) = f(a, rb)$ ($r \in R$).

We will construct an abelian group $A \otimes_R B$, called the tensor product of A and B over R, together with an R-biadditive map

$$\varphi\colon A \times B \to A \otimes_R B$$

that will have the following property.

For every abelian group H, and an R-biadditive map $f\colon A \times B \to H$, there is a unique group homomorphism $g\colon A \otimes_R B \to H$ such that the following diagram commutes:

$$\begin{tikzcd} A \times B \arrow[r] \arrow[dr, "f"'] & A \otimes_R B \arrow[d, "g"] \\ & H. \end{tikzcd}$$

Moreover, we shall show that if ${}_SA_R$ then $A \otimes_R B$ is a module in ${}_{\mathbf{S}}\mathbf{Mod}$ and, moreover,

$$A \otimes_R (-)\colon {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{S}}\mathbf{Mod},$$

is a covariant functor. On the other hand,

$$\mathrm{Hom}_S(A, -)\colon {}_{\mathbf{S}}\mathbf{Mod} \to {}_{\mathbf{R}}\mathbf{Mod},$$

is another covariant functor, and we shall show that

$$(A \otimes_R (-), \mathrm{Hom}_S(A, -)),$$

is an adjoint pair. Namely, for ${}_RB$, ${}_SC$ we have

$$\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(B, \mathrm{Hom}_S(A, C)).$$

A related result, less useful to us later, is that for A_R, ${}_RB_S$, C_S, we have $\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$. Namely, that

$$((-) \otimes_R B, \mathrm{Hom}_S(B, -))$$

is an adjoint pair.

2.4. Construction of $A \otimes_R B$.

We begin by constructing the free abelian group

$$G = \oplus_{(a,b) \in A \times B} \mathbb{Z}(a, b),$$

and we construct $A \otimes_R B$ as a quotient group. An element of G can be written as a finite sum $\sum_i n_i(a_i, b_i)$ with $n_i \in \mathbb{Z}$, $(a_i, b_i) \in A \times B$. Let N be the subgroup generated by all elements of G of the form

$$(a + a', b) - (a, b) - (a', b), \quad (a, b + b') - (a, b) - (a, b'), \qquad (ar, b) - (a, rb),$$

for any $a, a' \in A, b, b' \in B, r \in R$. (Note that, in particular, it contains elements such as $2(a, b) - (2a, b)$ and, more generally arguing by induction, also $n(a, b) - (na, b)$ for every $n \in \mathbb{Z}$.) We define then the **tensor product** of A and B over R as

$$A \otimes_R B = G/N.$$

The image of (a, b) in $A \otimes_R B$ is denoted $a \otimes b$. A general element of $A \otimes_R B$ is thus of the form

$$\sum_{i=1}^{n} a_i \otimes b_i$$

(one uses the comment concerning $n(a, b) - (na, b)$ to avoid writing coefficients in front of the $a_i \otimes b_i$). However, it is important to remember that in general this representation is not unique; for example, $(a + a') \otimes b = a \otimes b + a' \otimes b$. Therefore, care has to be taken when defining functions $A \otimes_R B \to C$ into an abelian group C by specifying their values on elements of the form $a \otimes b$ and claiming that they "extend by linearity". Such "functions" may not be well-defined. Before getting to that, though, we note that in $A \otimes_R B$ the following relations hold:

(1) $(a + a') \otimes b = a \otimes b + a' \otimes b$, for $a, a' \in A, b \in B$;
(2) $a \otimes (b + b') = a \otimes b + a \otimes b'$, for $a \in A, b, b' \in B$;
(3) $ar \otimes b = a \otimes rb$, for $a \in A, b \in B, r \in R$.

These identities are the content of the first claim in the following proposition.

Proposition 2.4.1. *The map*

$$A \times B \to A \otimes_R B, \quad (a, b) \mapsto a \otimes b,$$

is R-biadditive. $A \otimes_R B$ has the universal property that for every abelian group H and an R-biadditive map $f \colon A \times B \to H$ there is a unique group homomorphism $g \colon A \otimes_R B \to H$ such that the following diagram commutes:

$$\begin{tikzcd}
A \times B \arrow[r, "(biadd.)"] \arrow[rd, "f", "(biaddi.)"'] & A \otimes_R B \arrow[d, "g"', "(homomor.)"] \\
 & H.
\end{tikzcd}$$

Proof. We are given H and f and we wish to construct $g \colon A \otimes_R B \to H$ such that the diagram will commute. Certainly, for commutation to hold we must have $g(a \otimes b) = f(a, b)$. We would like to define then $g(\sum_{i=1}^{n} a_i \otimes b_i) = \sum_{i=1}^{n} f(a_i, b_i)$ and that is the only possibility for g. However, remembering that a representation of an element of $A \otimes_R B$ is not unique, this is problematic. What we do, and (generally speaking) this is what one *always* does, is to construct a homomorphism $\tilde{g} \colon G = \oplus_{(a,b) \in A \times B} \mathbb{Z}(a, b) \to C$ and use the first isomorphism theorem to define g.

As G is a free group, we can define $\tilde{g}(a, b) = f(a, b)$ and extend it by linearity. That is

$$\tilde{g}(\sum n_i(a_i, b_i)) = \sum n_i f(a_i, b_i).$$

(Note that we should have written $f((a_i, b_i))$, but it is better to drop a pair of paranthesis.) It is easy to check that $\tilde{g}$ is a homomorphism – this doesn't even require that f is a R-biadditive. To show that $N \subseteq \mathrm{Ker}(\tilde{g})$ we only need to check on generators of N and here we use that f is biadditive.

(1) $\tilde{g}((a + a', b) - (a, b) - (a', b)) = f(a + a', b) - f(a, b) - f(a', b) = 0.$
(2) $\tilde{g}((a, b + b') - (a, b) - (a, b')) = f(a, b + b') - f(a, b) - f(a, b') = 0.$
(3) $\tilde{g}((ar, b) - (a, rb)) = f(ar, b) - f(a, rb) = 0.$

Therefore, by the first isomorphism theorem for groups, there is a well defined group homomorphism

$$g \colon A \otimes_R B \to H, \qquad g(\sum_{i=1}^{n} a_i \otimes b_i) = \sum_{i=1}^{n} f(a_i, b_i).$$

It is clear that the diagram commutes. □

2.5. **Functorial properties.** The construction of $A \otimes_R B$ is functorial in the following sense.

Proposition 2.5.1. *Given $A_R, A'_R, {}_RB, {}_RB'$ and homomorphisms of modules,*

$$f\colon A \to A', \quad g\colon B \to B',$$

there is a unique group homomorphism

$$f \otimes g\colon A \otimes_R B \to A' \otimes_R B',$$

such that

$$(f \otimes g)(\sum a_i \otimes b_i) = \sum f(a_i) \otimes g(b_i).$$

Proof. Consider the map

$$f \times g\colon A \times B \to A' \otimes_R B', \qquad (a, b) \mapsto f(a) \otimes g(b).$$

It is an R-biadditive map. It therefore induces a group homomorphism

$$f \otimes g\colon A \otimes_R B \to A' \otimes_R B'$$

that satisfies $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$. The general formula for $f \otimes g$ follows since it is a group homomorphism. □

The proposition gives rather quickly that if A, or B, have extra properties, so does $A \otimes_R B$. For example:

Corollary 2.5.2. *(1) For ${}_SA_R, {}_RB$, $A \otimes_R B$ is a left S-module.*
(2) For $A_R, {}_RB_S$, $A \otimes_R B$ is a right S-module.

Proof. (1) For every $s \in S$ the map $a \mapsto sa$ is an R-module homomorphism of A that we denote $[s]$. The proposition applied to $[s] \otimes Id$ provides a group homomorphism $A \otimes_R B \to A \otimes_R B$ and we define

$$s \cdot (\sum a_i \otimes b_i) := ([s] \otimes Id)(\sum a_i \otimes b_i) = \sum (sa_i) \otimes b_i.$$

The key is that this is a well-defined homomorphism of $A \otimes_R B$. Now that we have the formula, it is immediate to check that this makes $A \otimes_R B$ into a left S-module. The proof of the second claim is essentially identical. □

Let R be a ring. A ring A is called an R**-algebra** if there is a ring homomorphism $\iota_A\colon R \to A$ whose image contained in the centre of A. Namely, if for all $r \in R, a \in A$ we have $\iota_A(r) \cdot a = a \cdot \iota_A(r)$. A morphism of R-algebras A, B, is a homomorphism of rings $f\colon A \to B$ such that $f(\iota_A(r)) = \iota_B(r)$. We get a category ${}_{\mathbf{R}}\mathbf{Alg}$.

Corollary 2.5.3. *If A_R, ${}_RB$ are R-algebras then $A \otimes_R B$ is an R-algebra.*

Proof. We need to define multiplication on $A \otimes_R B$. For $s \in A$ ($t \in B$) the map $[s](x) = sx$ (resp. $[t](x) = tx$, sic!) are R-modules homomorphisms and so we get a well-defined homomorphism of groups

$$([s] \otimes [t])(\sum a_i \otimes b_i) = \sum (sa_i) \otimes (tb_i).$$

Note that this provides an R-biadditive map $A \times B \to \mathrm{End}(A \otimes_R B)$ sending (s, t) to the homomorphism $[s] \otimes [t]$. By the universal property, we get a homomorphism

$$A \otimes_R B \to \mathrm{End}(A \otimes_R B), \qquad \sum s_i \otimes t_i \mapsto \sum [s_i] \otimes [t_i].$$

We define now a product on $A \otimes_R B$ by

$$(\sum s_i \otimes t_i) \cdot (\sum a_j \otimes b_j) := (\sum [s_i] \otimes [t_i])(\sum a_j \otimes b_j) = \sum_{i,j} s_i a_j \otimes t_i b_j.$$

The key is that this is a well-defined formula. Once we have it, it is straightforward to verify that this makes $A \otimes_R B$ into a ring. Eventually, we have the formula

$$s \otimes t \cdot a \otimes b = sa \otimes tb,$$

and multiplication of general elements proceeds by distributivity, but without the argument above it is not clear that this is well-defined.

We define a homomorphism $R \to A \otimes_R B$ by $r \mapsto \iota_A(r) \otimes 1 = 1 \otimes \iota_B(r)$. It is easy to check that this is a ring homomorphism and that the image of R is contained in the centre of $A \otimes_R B$. □

2.6. **Examples.**

Proposition 2.6.1. *Let R be a ring and ${}_RM$ a module. Then*

$$R \otimes_R M \cong M.$$

Proof. Define a function $M \to R \otimes_R M$ by $m \mapsto 1 \otimes m$. It is clearly a homomorphism of groups. On the other hand, define a map $R \times M \to M$ that takes (r, m) to rm. It is an R-biadditive map and so defines a group homomorphism

$$R \otimes M \to M, \qquad \sum r_i \otimes m_i \mapsto \sum r_i m_i.$$

These maps are mutual inverses. □

Proposition 2.6.2. *Let k be a commutative ring then*

$$k[x_1, \dots, x_m] \otimes_k k[y_1, \dots, y_n] \cong k[x_1, \dots, x_m, y_1, \dots, y_n].$$

Proof. Note that both sides are commutative k-algebras. As $k[x_1, \dots, x_m, y_1, \dots, y_n]$ is a free polynomial ring, we can define a homomorphism of it into any commutative k-algebra, uniquely, by specifying the images of the x_i and y_j. In particular, we get a homomorphism of k-algebras,

$$k[x_1, \dots, x_m, y_1, \dots, y_n] \to k[x_1, \dots, x_m] \otimes_k k[y_1, \dots, y_n],$$

by

$$x_i \mapsto x_i \otimes 1, \quad y_j \mapsto 1 \otimes y_j.$$

On the other hand, the map

$$k[x_1, \dots, x_m] \times_k k[y_1, \dots, y_n] \to k[x_1, \dots, x_m, y_1, \dots, y_n], \quad (f(x), g(y)) \mapsto f(x) \cdot g(y),$$

is a k-biadditive map and so induces a homomorphism (in fact, of k-algebras),

$$k[x_1, \dots, x_m] \otimes_k k[y_1, \dots, y_n] \to k[x_1, \dots, x_m, y_1, \dots, y_n]$$

that takes $f(x) \otimes g(y)$ to $f(x)g(y)$. In particular, it takes $x_i \otimes 1$ to x_i and $1 \otimes y_j$ to y_j. Using this map, we easily check that the homomorphisms we constructed between $k[x_1, \dots, x_m] \otimes_k k[y_1, \dots, y_n]$ and $k[x_1, \dots, x_m, y_1, \dots, y_n]$ are mutual inverses as it is enough to check that on the x_i and y_j. □

A similar argument proves that

$$(k[x_1, \dots, x_m]/I) \otimes_k (k[y_1, \dots, y_n]/J) \cong k[x_1, \dots, x_m, y_1, \dots, y_n]/(\langle I \rangle + \langle J \rangle),$$

where by $\langle I \rangle$ and $\langle J \rangle$ on the right hand side we mean the ideals generated by I and J, respectively, in $k[x_1, \dots, x_m, y_1, \dots, y_n]$.[3] So, for example,

$$\mathbb{Q}[x]/(x^2 - 2) \otimes_{\mathbb{Q}} \mathbb{Q}[y]/(y^2 - 2) \cong \mathbb{Q}[x, y]/(x^2 - 2, y^2 - 2).$$

The right hand side is a $\mathbb{Q}$-algebra but is not a field anymore. Indeed, it has zero divisors:

$$(x + y)(x - y) = x^2 - y^2 = 2 - 2 = 0$$

in this ring.

[3] If k is a field, an **affine k-variety** V is defined in algebraic geometry as a closed subset of k^m for some integer m. Per definition, such an object is defined by an ideal I of $k[x_1, \dots, x_m]$ – the equations defining V and the **regular functions** on V are defined as $k[x_1, \dots, x_m]/I$. The product of two varieties $V \subset k^m$, $W \subset k^n$, which is the same as their fibre product over a point, is a closed variety in k^{m+n} defined by the equations $\langle I \rangle + \langle J \rangle$ and its ring of regular functions is $k[x_1, \dots, x_m, y_1, \dots, y_n]/(\langle I \rangle + \langle J \rangle)$.

Proposition 2.6.3. *Let R be a commutative ring and I, J ideals of R then*[4]

$$R/I \otimes_R R/J \cong R/(I+J).$$

Proof. The method of proof is similar. Both sides are R-algebras. The map

$$R \mapsto R/I \otimes_R R/J, \qquad r \mapsto r \otimes 1,$$

is a homomorphism of rings. If $i \in I$ then $i \otimes 1 = 0 \otimes 1 = 0$ and if $j \in J$ then $j \otimes 1 = 1 \otimes j = 1 \otimes 0 = 0$. Thus, there is a well-defined homomorphism of rings

$$R/(I+J) \to R/I \otimes_R R/J, \qquad r \mapsto r \otimes 1.$$

On the other hand, the map

$$R/I \times R/J \to R/(I+J), \qquad (r,s) \mapsto rs,$$

is well-defined (because for $i \in I$, $(r,s) \equiv (r+i,s) \mapsto (r+i)s \equiv rs + is \equiv rs$ etc.) and is R-biadditive. It induces a homomorphism

$$R/I \otimes R/J \to R/(I+J), \quad \sum r_i \otimes s_i \mapsto \sum r_i s_i.$$

It is the inverse of the previous map because $r \mapsto r \otimes 1 \mapsto r$ in one direction, and in the other direction $\sum r_i \otimes s_i \mapsto \sum r_i s_i \mapsto \sum r_i s_i \otimes 1 = \sum r_i \otimes s_i$. □

Thus, for example,

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\gcd(m,n)\mathbb{Z},$$

and, in particular, the tensor product of two non-zero modules can be zero. For example,

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/\gcd(2,3)\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = 0.$$

2.7. Hom **and** $\otimes$ **are adjoint.**

Here is the example that motivates us. Let k be a field. Let G be a group and H a subgroup of G. Suppose that V is a left $k[H]$-module. As we shall explain later, this means exactly that V is a linear representation of H. Since $k[G]$ is a right $k[H]$-module, we can form

$$k[G] \otimes_{k[H]} V,$$

which is a left $k[G]$-module as $k[G]$ itself is a left $k[G]$-module in the obvious way. Thus, we get from a representation of H a representation of G, called the **induced representation** (and the process is called **induction**) and denoted by

$$\mathrm{Ind}_H^G V.$$

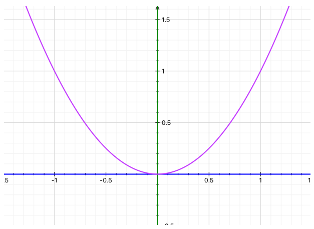
This is a very powerful method of creating representations of a "big" group G starting from a representation of a "small" subgroup H. In fact, this is a functor

$$\mathrm{Ind}_H^G \colon {}_{\mathbf{k[H]}}\mathbf{Mod} \to {}_{\mathbf{k[G]}}\mathbf{Mod}.$$

On the other hand, if W is a $k[G]$-module, since $k[H] \subseteq k[G]$ we can forget about $k[G]$ and view it only as a $k[H]$-module. This way we get a **restriction** functor

$$\mathrm{Res}_H^G \colon {}_{\mathbf{k[G]}}\mathbf{Mod} \to {}_{\mathbf{k[H]}}\mathbf{Mod}.$$

[4] In algebraic geometry the **intersection** of two varieties $V, W \subset k^n$ is the same as their fibre product over k^n and this is defined algebraically as $k[x_1,\dots,x_n]/I \otimes_{k[x_1,\dots,x_n]} k[x_1,\dots,x_n]/J = k[x_1,\dots,x_n]/(I+J)$. So, for example, the intersection of the parabola $y = x^2$ with the line $x = 0$ is defined by the ideal $\langle y - x^2, x\rangle = \langle y, x\rangle$ corresponding to the point 0. On the other hand, the intersection of the parabola with the line $y = 0$ is defined by the ideal $\langle y - x^2, y\rangle = \langle y, x^2\rangle$ that corresponds, in some sense, to the point 0 with multiplicity 2. This reflects the fact that the line $y = 0$ is tangent to the parabola, while the line $x = 0$ is transversal.



We shall prove that $(\mathrm{Ind}_H^G, \mathrm{Res}_H^G)$ is an adjoint pair. That means that for every $k[G]$-module W and every $k[H]$-module V we have

$$\mathrm{Hom}_{k[G]}(\mathrm{Ind}_H^G V, W) \cong \mathrm{Hom}_{k[H]}(V, \mathrm{Res}_H^G W),$$

where the right hand side means homomorphisms of $k[H]$-modules from V to W, forgetting that W has a richer structure of a $k[G]$-module. This is a form of **Frobenius reciprocity**, which we will prove in more precise form later. This allows us to investigate the new representation $\mathrm{Ind}_H^G V$, using the representation theory of H that we might already understand well. Instead of dealing with this example only, with the same effort we can prove a more general result.

Theorem 2.7.1. *Let R, S be rings and ${}_S A_R$ be a bimodule. Then,*

$$A \otimes_R (-) \colon {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{S}}\mathbf{Mod}, \qquad \mathrm{Hom}_S(A, -) \colon {}_{\mathbf{S}}\mathbf{Mod} \to {}_{\mathbf{R}}\mathbf{Mod}$$

are covariant functors. The pair

$$(A \otimes_R (-), \mathrm{Hom}_S(A, -)),$$

is an adjoint pair. Namely, for ${}_R B$, ${}_S C$ we have

$$\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(B, \mathrm{Hom}_S(A, C)).$$

Proof. Given $f \in \mathrm{Hom}_S(A \otimes_R B, C)$ define $\phi \in \mathrm{Hom}_R(B, \mathrm{Hom}_S(A, C))$ by sending b to

$$\phi_b \colon A \to C, \quad \phi_b(a) = f(a \otimes b).$$

On the other hand, given $\phi \in \mathrm{Hom}_R(B, \mathrm{Hom}_S(A, C))$ say $b \mapsto \phi_b \in \mathrm{Hom}_S(A, C)$, define

$$f \colon A \otimes_R B \to C, f(a \otimes b) = \phi_b(a).$$

We need to check that everything is well-defined and the maps are maps of modules, as required. We begin with f. The function $\phi_b(a) = f(a \otimes b)$ is a function from A to C that is a map of S-modules in the variable a, because f satisfies $f(sa \otimes b) = sf(a \otimes b)$ and is linear in a. Further, we have the formulas:

$$\phi_{b+b'} = \phi_b + \phi_{b'}, \quad \phi_{rb} = r\phi_b,$$

because, recall, $(r\phi_b)(a) := \phi_b(ar) = f(ar \otimes b) = f(a \otimes rb) = \phi_{rb}(a)$. So the ϕ associated to f is in $\mathrm{Hom}_R(B, \mathrm{Hom}_S(A, C))$. Finally, denoting now $\phi = \phi(f)$ we need to still verify that $\phi(f + f') = \phi(f) + \phi(f')$, because the isomorphism in the theorem should be an isomorphism of groups. This is easy to check (one needs to check that for every b the functions $A \to C$ given by $\phi(f + f')_b$ and $\phi(f)_b + \phi(f')_b$ are the same).

The converse goes rather similarly. The only point to be careful about is that starting from ϕ the definition of $f \colon A \otimes_R B \to C, f(a \otimes b) = \phi_b(a)$ is a good definition. One starts, as usual, by arguing that $A \times B \to C$, given by $(a, b) \mapsto \phi_b(a)$ is an R-biadditive function. Having proven that, one gets that f is well-defined and proceeds to show it is S-linear and that associating f to ϕ is a homomorphism.

Of course, we are not done. One needs to check that these isomorphisms are natural relative to maps $B \to B', C \to C'$. We leave that as an exercise. □

Corollary 2.7.2. *Let $R = k[H], S = k[G]$, V a left $k[H]$-module and W a left $k[G]$-module. Then*

$$\mathrm{Hom}_{k[G]}(k[G] \otimes_{k[H]} V, W) \cong \mathrm{Hom}_{k[H]}(V, W).$$

Or, in slightly different notation,

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G V, W) \cong \mathrm{Hom}_H(V, \mathrm{Res}_H^G W).$$

Proof. Indeed, taking in the Theorem the ring $A = k[G]$ the result follows if we use the isomorphism $\mathrm{Hom}_{k[G]}(k[G], W) \cong W$ (see Example 2.1.1). □

Part 3. **Complex representations of finite groups**

3. Definitions and basic examples

3.1. **Basic definitions and conventions.** *In this part of the notes, a vector space V would always denote a finite dimensional vector space over the complex numbers.* If V, W, are vector spaces then $\mathrm{Hom}(V,W)$ denotes the $\mathbb{C}$-linear maps $T\colon V \to W$; $\mathrm{Hom}(V,W)$ is a $\mathbb{C}$-vector space whose dimension is $\dim(V)\cdot\dim(W)$. A particular case is $\mathrm{End}(V) := \mathrm{Hom}(V,V)$, which is not just a $\mathbb{C}$-vector space of dimension $\dim(V)^2$, but in fact a $\mathbb{C}$-algebra under addition of linear maps and where multiplication is given by composition of maps. By $\mathrm{Aut}(V)$, or $\mathrm{GL}(V)$, we mean the invertible elements of $\mathrm{End}(V)$, namely, all the invertible linear transformations $T\colon V\to V$. *Throughout, G denotes a finite group.*

The main definition of this part of the course is the following:

Definition 3.1.1. A finite dimensional **linear representation** of G is a homomorphism

$$\rho\colon G \to \mathrm{Aut}(V),$$

for some finite dimensional complex vector space V.

We will usually just say "representation" and not "finite-dimensional linear representation", which is a bit of a mouthful. Note that a representation of G is really two pieces of data:

(1) ρ (the homomorphism), and
(2) V (the vector space on which G acts through ρ).

And so, we will often say that (ρ, V) is a representation of G. Also note that when we are given a representation, the group G acts on the set V in the sense of group actions on sets, albeit in a very particular way – through linear invertible transformations.

Definition 3.1.2. A **morphism of representations** $T\colon (\rho_1, V_1) \to (\rho_2, V_2)$ is a linear map

$$T\colon V_1 \to V_2,$$

such that

$$\rho_2(g)\circ T = T\circ\rho_1(g), \qquad \forall g\in G.$$

In diagram: for all $g \in G$, the following diagram commutes:

$$\begin{tikzcd} V_1 \arrow[r, "\rho_1(g)"] \arrow[d, "T"'] & V_1 \arrow[d, "T"] \\ V_2 \arrow[r, "\rho_2(g)"] & V_2. \end{tikzcd}$$

An **isomorphism of representations** is therefore such a bijective T.

There is therefore an *important distinction*. Even if V_1, V_2 are representations of G we use $\mathrm{Hom}(V_1, V_2)$ to denote the linear maps from V_1 to V_2. We shall use

$$\mathrm{Hom}_G(V_1, V_2)$$

to denote the morphisms of representations $(\rho_1, V_1) \to (\rho_2, V_2)$. It is a *subspace* of $\mathrm{Hom}(V_1, V_2)$ (and more on that below). A more accurate notation for $\mathrm{Hom}_G(V_1,V_2)$ is $\mathrm{Hom}_G((\rho_1,V_1),(\rho_2,V_2))$ but we shall avoid it if we can, because it is harder to read.

We have, in fact, defined a category $\mathbf{Rep(G)}$ of finite-dimensional representations of G.

Lemma 3.1.3. *The category $\mathbf{Rep(G)}$ is equivalent to the category ${}_{\mathbb{C}[\mathbf{G}]}\mathbf{Mod}$.*

Before proving the lemma we need to explain some concepts from category theory. Two categories $\mathbf{C}, \mathbf{D}$ are called **equivalent** if there are covariant functors

$$F\colon \mathbf{C} \to \mathbf{D}, \quad G\colon \mathbf{D} \to \mathbf{C},$$

such that

$$G \circ F \cong \mathbb{1}_{\mathbf{C}}, \qquad F \circ G \cong \mathbb{1}_{\mathbf{D}},$$

where $\mathbb{1}_{\mathbf{C}}, \mathbb{1}_{\mathbf{D}}$ are the identity functors. The functors F, G are then called an **equivalence**. If both functors are contravariant, we call this an **anti-equivalence**. Note that we do not require that $G \circ F = \mathbb{1}_{\mathbf{C}}$ and $F \circ G = \mathbb{1}_{\mathbf{D}}$., but if actual equality holds then the categories are surely equivalent. We will come back to these concepts and provide more examples when we discuss Morita equivalence.

Sometimes the categories have more structure and then we want to demand that an equivalence preserves them. A category is called **pre-additive** if all the morphism sets $\mathrm{Mor}(A, B)$ are abelian groups and composition respects the group structure: $g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$ and $(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$. The main example is the category ${}_{\mathbf{R}}\mathbf{Mod}$ of R-modules.

When we consider functors between pre-additive categories we usually require then to respect the group structure. Naturally, they are called **additive functors**. Namely, if $f_1, f_2 \in \mathrm{Mor}(A, B)$ then $F(f_1 + f_2) = Ff_1 + Ff_2$ in $\mathrm{Mor}(FA, FB)$. The lemma claims that the two pre-additive categories, $\mathbf{Rep}(\mathbf{G})$ and ${}_{\mathbb{C}[\mathbf{G}]}\mathbf{Mod}$, are equivalent.

Proof. Given a $\mathbb{C}[G]$-module V, where we write $\alpha \cdot v$ for $\alpha \in \mathbb{C}[G], v \in V$, to denote the module structure. Define a map,

$$\rho\colon G \to \mathrm{Aut}(V), \qquad \rho(g)(v) := g \cdot v.$$

The map $\rho(g)$ is $\mathbb{C}$-linear because we have $\rho(g)(v_1 + v_2) = g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2 = \rho(g)(v_1) + \rho(g)(v_2)$. Also, if $a \in \mathbb{C}$, by definition $a \cdot v$ is the structure of V as a $\mathbb{C}$-module. Then $\rho(g)(k \cdot v) = gk \cdot v = kg \cdot v = k \cdot \rho(g)(v)$, using that $\mathbb{C}$ is in the centre of $\mathbb{C}[G]$. Thus, $\rho(g) \in \mathrm{End}_{\mathbb{C}}(V)$. Also,

$$\rho(g_1 g_2)(v) = (g_1 g_2) \cdot v = g_1 \cdot (g_2 \cdot v) = (\rho(g_1) \circ \rho(g_2))(v).$$

This shows that ρ is a homomorphism of groups. In particular, each $\rho(g)$ is invertible and so we have a homomorphism

$$\rho\colon G \to \mathrm{Aut}(V).$$

Conversely, given $\rho\colon G \to \mathrm{Aut}(V)$, define

$$(\sum a_g g) \cdot v = \sum_g a_g \rho(g)(v).$$

It is straightforward to verify this makes V into a left $\mathbb{C}[G]$-module.

At this point, we of course need to define what happens to morphisms. If T is a morphism of G-representations, it follows from the formula above that T commutes with $\mathbb{C}[G]$-module structure. Indeed, $T((\sum a_g g) \cdot v) = T(\sum_g a_g \rho_1(g)(v)) = \sum_g a_g T(\rho_1(g)(v)) = \sum_g a_g \rho_2(g)(Tv) = (\sum_g a_g g)(Tv)$. It is equally easy to check that a map of $\mathbb{C}[G]$-modules is a map of G-representations.

We have thus constructed functors in both directions. In fact, functors that do not change the objects or the morphisms. And so it is clear the functors are inverses of one another, and the categories are equivalent. □

Let (ρ, V) be a representation of G. A **subrepresentation** is a subspace $W \subseteq V$ such that for all $g \in G$ we have

$$\rho(g)(W) \subseteq W.$$

In fact, we then have necessarily $\rho(g)(W) = W$ because also $\rho(g^{-1})(W) \subseteq W$ and therefore $\rho(g)\rho(g^{-1})W \subseteq \rho(g)W$ and we get $W \subseteq \rho(g)W$. In that case $(\rho|_W, W)$ is a representation and the inclusion map $(\rho|_W, W) \to (\rho, V)$ is a morphism of representations. Note that V and $\{0\}$ are always sub-representations and we shall refer to them as **trivial sub-representations**.

If $W \subset V$ is a sub-representation then the quotient space V/W is a representation $\bar{\rho}$ of G as well, where we define

$$\bar{\rho}(g)(v+W) = \rho(g)(v) + W, \qquad g \in G, v \in V.$$

It is called a **quotient representation**. Note that a subrepresentation, or a quotient representation, is nothing else than a $\mathbb{C}[G]$-submodule, or a quotient module, respectively.

The following definition is one of the key concepts.

Definition 3.1.4. A representation (ρ, V) is called **irreducible** if $V \neq \{0\}$ and its only sub-representations are the trivial ones.

3.2. **Direct sum and** Hom**.** Let G be a group and $(\rho, V), (\tau, W)$ be two representations of G. Then

$$(\rho \oplus \tau, V \oplus W)$$

is a representation of G where

$$(\rho \oplus \tau)(g) = (\rho(g), \tau(g)).$$

This representation is called the **direct sum representation**. If we wish, we can also use the notation $\rho(g) \oplus \tau(g)$, which we have used before for the direct sum of two linear maps. We will often be rather loose with our notation and write either $V \oplus W$, or $\rho \oplus \tau$, for the direct sum. Similarly, we shall write the direct sum of (ρ, V) with itself a-times as either $(\rho, V)^a$, V^a or ρ^a.

Another construction we have is $\mathrm{Hom}((\rho, V), (\tau, W))$. Let us denote this representation by

$$\sigma \colon G \to \mathrm{Aut}(\mathrm{Hom}(V, W)),$$

where for every $g \in G$, $T \colon V \to W$,

$$\sigma(g)(T) := \tau(g) \circ T \circ \rho(g^{-1}).$$

There is actually quite a bit to verify here. We only indicate what should be verified and leave the verification as an exercise.

- As $\mathrm{Hom}(V, W)$ is a complex vector space, we need to verify that for every $g \in G$, $\sigma(g)$ is an endomorphism of that space. Namely, that indeed $\tau(g) \circ T \circ \rho(g^{-1})$ is a linear map from V to W, and that
$$T \mapsto \tau(g) \circ T \circ \rho(g^{-1}),$$
is linear in T. This just establishes that $\sigma(g)$ is a linear endomorphism of the vector space $\mathrm{Hom}(V, W)$.
- Next, one needs to verify that $\sigma(gh) = \sigma(g) \circ \sigma(h)$. This shows that we have a multiplicative map $G \to \mathrm{End}(\mathrm{Hom}(V, W))$. But note that, since every element in G is invertible and $\sigma(1)$ is the identity map, automatically $\sigma(g)$ is invertible, because $\sigma(g) \circ \sigma(g^{-1}) = \sigma(1) = Id$, etc. Thus, it follows that we get a homomorphism
$$\sigma \colon G \to \mathrm{Aut}(\mathrm{Hom}(V, W)).$$

3.3. **The trivial subrepresentation.** Let (ρ, V) be a representation of G and let

$$V^G := \{v \in V : \rho(g)(v) = v, \forall g \in G\}.$$

This is the space of invariant vectors. Note that V^G is a sub-representation of V on which G acts trivially; it is called the **trivial subrepresentation** of V. The homomorphism

$$G \to \mathrm{Aut}(V^G),$$

induced from ρ is simply $g \mapsto Id, \forall g \in G$. Note that

$$\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G.$$

Unfortunately, at this point we have two conflicting meanings for "trivial subrepresentation of V". One we have just discussed. It is V^G, and the choice of name is because G acts trivially on V^G. The other was previously used to refer to $\{0\}$ and V as trivial subrepresentations, because they always exist and there is nothing deep about their existence. We will make efforts to clarify which way we are using "trivial subrepresentation" whenever confusion is possible.

Remark 3.3.1. The construction $\mathrm{Hom}(V, W)$, besides its theoretical usefulness that we shall see repeatedly below, is a very good way to construct representations. For example, if W is a representation and V is a one dimensional representation then $\mathrm{Hom}(V, W)$ is another representation of the same dimension as W. In fact, if W is irreducible, it will be the case that $\mathrm{Hom}(V, W)$ is irreducible too, but that requires a proof; it would be much easier to give once we have the main theorems available. It may be the case that $\mathrm{Hom}(V, W) \cong W$ as representations, but often this is not the case, and so, once we have constructed an irreducible representation W, we are often able to construct more of them as $\mathrm{Hom}(V, W)$, for various 1-dimensional representations V.

Lemma 3.3.2. *Let (ρ, V) be an irreducible representation then either $V^G = \{0\}$ or $V = V^G$, and is then a one-dimensional space on which G acts trivially.*

Proof. As V^G is a sub-representation and V is irreducible, either $V^G = \{0\}$ or $V^G = V$. In the latter case, let $v \in V$ be a non-zero vector. Then $\mathrm{Span}_{\mathbb{C}}(v)$ is a subrepresentation and consequently $V = \mathrm{Span}_{\mathbb{C}}(v)$, hence a one-dimensional space. □

3.4. **Examples of representations.**

3.4.1. *Passing to coordinates.* Let

$$\rho \colon G \to \mathrm{GL}_n(\mathbb{C})$$

be a homomorphism of groups. Then $(\rho, \mathbb{C}^n)$ is a representation as we have a canonical identification

$$\mathrm{GL}_n(\mathbb{C}) = \mathrm{Aut}(\mathbb{C}^n),$$

by sending every linear map T to the matrix $[T]_{St}$ representing it in the standard basis.

More generally, let V be an n-dimensional vector space and (ρ, V) a representation of G. Let B be a basis for V. We get then

$$T \colon (\rho, V) \cong (\tau, \mathbb{C}^n),$$

where $T \colon V \to \mathbb{C}^n$ is the map sending v to $[v]_B$ and

$$\tau(g) = [\rho(g)]_B.$$

The identity $T \circ \rho(g) = \tau(g) \circ T$, namely, for all $v \in V$, $T \circ \rho(g)(v) = \tau(g) \circ T(v)$ translates in this case to the identity $[\rho(g)(v)]_B = [\rho(g)]_B[v]_B$, which is precisely the property defining the matrix $[\rho(g)]_B$.

Thus, up to isomorphism, all linear representations can be viewed as group homomorphisms $G \to \mathrm{GL}_n(\mathbb{C})$. However, this perspective is not canonical. If we choose another basis C we get a different representation

$$\tau' \colon G \to \mathrm{GL}_n(\mathbb{C}), \quad \tau'(g) = [\rho(g)]_C.$$

The two representations are isomorphic

$$(\tau, \mathbb{C}^n) \cong (\tau', \mathbb{C}^n)$$

via the change of basis matrix ${}_C M_B$ that may be viewed as an isomorphism

$${}_C M_B \colon \mathbb{C}^n \to \mathbb{C}^n;$$

Indeed, we have

$$\tau'(g)\ {}_C M_B = {}_C M_B\ \tau(g).$$

In particular, if we choose to view representations of G as homomorphisms

$$\rho\colon G \to \mathrm{GL}_n(\mathbb{C}),$$

then the isomorphism class of ρ are the homomorphisms

$$\rho^M\colon G \to \mathrm{GL}_n(\mathbb{C}), \quad \rho^M(g) := M\rho(g)M^{-1},$$

for any $M \in \mathrm{GL}_n(\mathbb{C})$.

3.4.2. *The standard representation of S_n.* We define the **standard representation** ρ^{st} of S_n by associating to $\sigma \in S_n$ the linear transformation given on the standard basis by

$$e_i \mapsto e_{\sigma(i)}.$$

In matrices $\sigma \mapsto M_\sigma$, where M_σ is the matrix whose $(\sigma(j), j)$ entry is 1 (for any j), and all the other entries are zero. Note, though, that

$$M_\sigma\ {}^t(x_1, \dots, x_n) = {}^t(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}).$$

To illustrate, for $n = 3$, we have the following matrices

$$M_1 = \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1 \end{pmatrix}, M_{(12)} = \begin{pmatrix} 0&1&0\\1&0&0\\0&0&1 \end{pmatrix}, M_{(123)} = \begin{pmatrix} 0&0&1\\1&0&0\\0&1&0 \end{pmatrix}.$$

The standard representation has two sub-representations

$$U_1 = \mathrm{Span}_{\mathbb{C}}\{(1, 1, \dots, 1)\}, \qquad U_0 = \{(x_1, \dots, x_n) : x_1 + \dots + x_n = 0\}.$$

In fact, let ρ^{st} denote the standard representation, let $\rho^{st}|_{U_1}, \rho^{st}|_{U_0}$, denote the sub-representations, then

$$\rho^{st} \cong \rho^{st}|_{U_1} \oplus \rho^{st}|_{U_0}.$$

Notation: We will denote $\rho^{st}|_{U_0}$ by $\rho^{St,0}$. And for any group G we will denote by $\mathbb{1}_G$ the trivial representation $G \to \mathbb{C}^\times$ taking every element of G to 1. Thus,

$$\rho^{St} = \mathbb{1}_{S_n} \oplus \rho^{St,0}.$$

Proposition 3.4.1. *Assume that $n \geq 2$. U_0 is an irreducible $n-1$ dimensional representation of S_n.*

Proof. We assume that $n \geq 3$. The case $n = 2$ is easy as U_0 is 1-dimensional.

Let $U' \subseteq U_0$ be a non-zero sub-representation. Let $x = (x_1, \dots, x_n)$ be a non-zero vector in U'. If x has precisely two non-zero elements, by multiplying x by a scalar we may assume that $x = (0, \dots, 0, 1, 0 \dots, 0, -1, 0, \dots, 0)$. Then, by acting by S_n we see that every vector of the form $e_i - e_j$ (where e_i are the standard basis) is also in U'. But these vectors span U_0 and it follows that $U' = U_0$.

Thus, it remains to prove that U' always contains such a vector. Let $x \in U'$ be a non-zero vector; it has more than one non-zero coordinate. If x has more than 2 non-zero coordinates, we show that there is vector $y \in U'$ that is not zero and has fewer non-zero coordinates.

Assume therefore that x has at least 3 non-zero coordinates. First, by rescaling we may assume that one of these coordinates is 1. Then, as $\sum x_i = 0$, there exists a non-zero coordinate that is not equal to 1. By applying a permutation to x we may assume that

$$x = (1, x_2, x_3, \dots, x_n),$$

where $x_2 \neq 1$ and is non-zero and also $x_3 \neq 0$. The vector

$$x' = \frac{1}{x_2}(x_2, 1, x_3, \dots, x_n),$$

also belongs to U'. Therefore, also

$$y = x - x' = (0, x_2 - \frac{1}{x_2}, x_3(1 - \frac{1}{x_2}), \dots, x_n(1 - \frac{1}{x_2})),$$

belongs to U' and this vector has fewer non-zero coordinates, yet is not zero (consider its third coordinate). □

3.4.3. *The regular representation.* This is one of the key examples, in fact. Using the language we have, it is easy to describe. It is simply $\mathbb{C}[G]$ considered as a left $\mathbb{C}[G]$-module! It is called the **regular representation** of G. Its dimension is the cardinality of G.

3.4.4. *One dimensional representations.* The one dimensional representations of a group G are, up to isomorphism, homomorphisms

$$G \to \mathbb{C}^\times.$$

They are of course all irreducible. Let

$$\hat{G} = \{\rho | \rho \colon G \to \mathbb{C}^\times \text{ homomorphism}\}.$$

Then $\hat{G}$ is an abelian group, called the **character group** of G, where the group operation is

$$(\rho \cdot \tau)(g) = \rho(g) \cdot \tau(g).$$

The identity is the trivial homomorphism $\mathbb{1}_G$ giving us the **trivial representation** $(\mathbb{1}_G, \mathbb{C})$, namely, $\mathbb{1}_G \colon G \to \mathbb{C}^\times, \mathbb{1}_G(g) = 1$ for all $g \in G$. The following are not too difficult to check:

- $\widehat{H \times G} \cong \hat{H} \times \hat{G}$ (canonically).
- $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$.
- Therefore, combining the two facts provided above, if G is a finite abelian group $\hat{G} \cong G$ (non-canonically).
- For a general group G, we have $\hat{G} = \widehat{G/G'}$, where G' is the commutator subgroup.
- In particular, for a general group G, $\hat{G}$ may be very small compared to G. For example, for $n \geq 5$ we have $\hat{A}_n = \{1\}, \hat{S}_n \cong \mathbb{Z}/2\mathbb{Z}$.

Given elements $\alpha_1, \dots, \alpha_n$ of $\hat{G}$ (any elements, repetitions allowed), we get an n-dimensional representation of G

$$g \mapsto \begin{pmatrix} \alpha_1(g) & & & \\ & \alpha_2(g) & & \\ & & \ddots & \\ & & & \alpha_n(g) \end{pmatrix}.$$

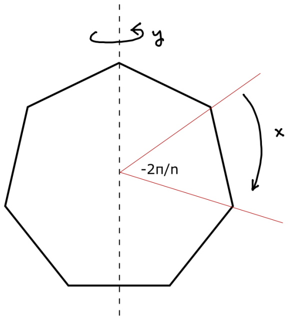
We leave it as an exercise to show that if G is an abelian group, any n-dimensional representation of G is isomorphic to such a representation. Thus, we know all the representations of finite abelian groups: Any irreducible representation is 1-dimensional, given by an element of $\alpha \in \hat{G}$. Any representation is isomorphic to a sum of 1-dimensional representations.

3.4.5. *A representation of D_n and A_4.* Let $n \geq 3$ and consider the dihedral group D_n generated by x, y. The symmetries of a regular n-gon in the plane, provided by elements of D_n, are naturally linear transformations of $\mathbb{R}^2$ and we can associate to x, y, the following matrices

$$x \mapsto \begin{pmatrix} \cos(2\pi/n) & \sin(2\pi/n) \\ -\sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \quad y \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We view these as complex matrices thereby obtaining a homomorphism

$$\rho^{plane} \colon D_n \to \mathrm{GL}_2(\mathbb{C}).$$



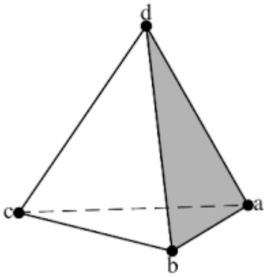
Another geometric example is the representation of A_4 coming from its action on a regular tetrahedron. We view A_4 as permuting the letters a, b, c, d, thereby acting by symmetries on the tetrahedron. This action comes from a linear representation

$$A_4 \to \mathrm{GL}_3(\mathbb{R}) \subseteq \mathrm{GL}_3(\mathbb{C}).$$

Although this representation certainly looks irreducible, and it is, one has to be careful. Also the action of $\mathbb{Z}/4\mathbb{Z}$ on $\mathbb{R}^2$, where $a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^a$ looks irreducible (and indeed, it cannot be decomposed as a *real* representation). But, viewed as a representation

$$\mathbb{Z}/4\mathbb{Z} \to \mathrm{GL}_2(\mathbb{C}),$$

it is reducible. Every representation of dimension greater than 1 of an abelian group is!



3.4.6. *Restriction and induction.* We have already seen in the language of modules, induction and restriction. If $H < G$ and V is a representation of G then $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ is a representation of G, called the induced representation $\mathrm{Ind}_H^G V$. Similarly, if W is a representation of G then W is also a representation of H denoted $\mathrm{Res}_H^G W$. Recall the adjoint property

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G V, W) = \mathrm{Hom}_H(V, \mathrm{Res}_H^G W).$$

Suppose that W is an irreducible representation of G and V is the trivial one dimensional representation of the trivial subgroup H. Then $\mathrm{Ind}_H^G V = \mathbb{C}[G]$ and $\mathrm{Hom}_H(V, \mathrm{Res}_H^G W) \neq 0$. Thus, there is a nonzero map of representations

$$T \colon \mathbb{C}[G] \to W.$$

As W is an irreducible G representation and the image of a map of G-representation is a subrepresentation (if you prefer, the image of a module homomorphism is a submodule), T must be surjective. We conclude that any irreducible representation of G is a quotient representation of $\mathbb{C}[G]$ and, in particular, its dimension is at most $|G|$. (It will follow from Theorem 5.1.2 that every irreducible representation of G is also a sub-representation of $\mathbb{C}[G]$.)

4. CHARACTERS

4.1. **The character of a representation.** Let (ρ, V) be a representation of G. Define the **character** of ρ, χ_ρ, by

$$\chi_\rho \colon G \to \mathbb{C}, \quad \chi_\rho(g) = \mathrm{Tr}(\rho(g)).$$

Here Tr denotes the trace of a square matrix, $\mathrm{Tr}(m_{ij}) = \sum m_{ii}$.

Lemma 4.1.1. *The function χ_ρ is well-defined and depends on ρ only up to isomorphism. Furthermore, χ_ρ is a* **class function** *on G. That is, for all $g, h \in G$, we have*

$$\chi_\rho(g) = \chi_\rho(hgh^{-1}).$$

In addition,

$$\chi_{\rho\oplus\tau} = \chi_\rho + \chi_\tau, \qquad \chi_\rho(1) = \dim(\rho), \qquad \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}.$$

(By $\dim(\rho)$ we mean the dimension of V where $\rho\colon G \to \mathrm{Aut}(V)$.)

Proof. By "well-defined" we mean that we have defined the trace of a linear transformation T as the trace of a matrix representing it in a given basis B. As the trace is independent of the choice of basis, χ_ρ is well-defined.

If $\rho \cong \tau$, then by choosing bases we may assume that

$$\rho\colon G \to \mathrm{GL}_n(\mathbb{C}), \quad \tau\colon G \to \mathrm{GL}_n(\mathbb{C}).$$

As invertible linear transformations $\mathbb{C}^n \to \mathbb{C}^n$ are represented by invertible matrices, the information that $\rho \cong \tau$ translates into the statement that there is an invertible matrix $M \in \mathrm{GL}_n(\mathbb{C})$ such that for all $g \in G$

$$M\rho(g)M^{-1} = \tau(g).$$

But then,

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)) = \mathrm{Tr}(M\rho(g)M^{-1}) = \mathrm{Tr}(\tau(g)) = \chi_\tau(g).$$

Actually, the same computation gives

$$\chi_\rho(hgh^{-1}) = \mathrm{Tr}(\rho(hgh^{-1})) = \mathrm{Tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{Tr}(\rho(g)) = \chi_\rho(g).$$

Therefore, χ_ρ is a class function.

Given representations $(\rho, V), (\tau, W)$, by choosing bases, we may assume that

$$\rho\colon G \to \mathrm{GL}_m(\mathbb{C}), \quad \tau\colon G \to \mathrm{GL}_n(\mathbb{C}),$$

and so

$$\rho \oplus \tau\colon G \to \mathrm{GL}_{m+n}(\mathbb{C}), \quad (\rho \oplus \tau)(g) = \begin{pmatrix} \rho(g) & 0 \\ 0 & \tau(g) \end{pmatrix}.$$

Therefore,

$$\chi_{\rho\oplus\tau}(g) = \mathrm{Tr}\begin{pmatrix} \rho(g) & 0 \\ 0 & \tau(g) \end{pmatrix} = \mathrm{Tr}(\rho(g)) + \mathrm{Tr}(\tau(g)) = \chi_\rho(g) + \chi_\tau(g).$$

Now, $\chi_\rho(1) = \mathrm{Tr}(I_n)$, where I_n is the $n \times n$ identity matrix and $n = \dim(V)$. Thus, $\chi_\rho(1) = \dim(\rho)$.

For the last property stated in the Lemma, fix the element g and let k be its order in the group G. Then, $\rho(g)^k = \rho(g^k) = \rho(1) = Id$. That means that $\rho(g)$ solves the polynomial $x^k - 1$, which has distinct roots, and so the minimal polynomial of g, which divides $x^k - 1$, also has distinct roots and therefore $\rho(g)$ is diagonalizable. And so, we may find a basis B of V in which

$$[\rho(g)]_B = \mathrm{diag}(\alpha_1, \dots, \alpha_n).$$

In addition, as $\rho(g)^k = I_n$, the α_i are roots of unity of order (dividing) n.

Note that the basis B is chosen specifically for g. There is no reason for $[\rho(h)]_B$ to be diagonal if $h \neq g$. However, because of the homomorphism property, one exception is that

$$\rho(g^{-1}) = \mathrm{diag}(\alpha_1^{-1}, \dots, \alpha_n^{-1}) = \mathrm{diag}(\bar{\alpha}_1, \dots, \bar{\alpha}_n),$$

where the second equality is a consequence of α_i being roots of unity. Therefore,

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}.$$

□

Characters are the heart of the whole story. Everything will be determined by characters.

For example, we will see that two representations are isomorphic if and only if they have the same character. Given an irreducible representation W we will be able to calculate, using characters, whether it appears as a subrepresentation of another representation V. And many other results.

Here are some examples of characters:

(1) For the standard representation of the symmetric group S_n we have
$$\chi_{\rho^{st}}(\sigma) = \mathrm{Tr}(\rho^{st}(\sigma)) = \text{ the number of fixed points of } \sigma.$$
(2) For the dihedral group D_n we have
$$\chi_{\rho^{plane}}(y) = 0, \qquad \chi_{\rho^{plane}}(x) = 2\cos(2\pi/n).$$
(3) If (ρ, V) is a trivial representation, namely $\rho(g) = Id$ for all $g \in G$, then χ_ρ is the constant function
$$\chi_\rho \equiv n,$$
where $n = \dim(V)$.

(4) Consider the 1-dimension sign representation of S_n given by
$$\mathrm{sgn}\colon S_n \to \{\pm 1\} \subset \mathbb{C}^\times.$$
Then $\chi_{\mathrm{sgn}}(\sigma) = +1$ if σ is an even permutation, and $\chi_{\mathrm{sgn}}(\sigma) = -1$, if σ is odd.

(5) If $\alpha \in \hat{G}$ is a 1-dimensional representation then χ_α is simply α.

4.2. **The character of an induced representation.** This is an important calculation. Let $H < G$ be groups and (ρ, V) a representation of H with character χ. We want to the determine the character of $\mathrm{Ind}_H^G V$ in terms of χ. We will denote it $\mathrm{Ind}_H^G \chi$.

Choose a set of coset representations $G = \coprod_{i=1}^d g_i H$. Then $\mathbb{C}[G] = \oplus_{i=1}^d g_i \mathbb{C}[H]$ as a right $\mathbb{C}[H]$-module and, as $\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V = V$, we have a decomposition
$$\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V = \bigoplus_{i=1}^d g_i \otimes V.$$
How does G act? Given $g \in G$, we have
$$g g_i = g_j h,$$
where j, and $h \in H$, depend on g and i. In fact, if we write $j = j(g,i), h = h(g,i)$, then for any fixed g the map $i \mapsto j(g,i)$ is a permutation of $\{1, \dots, d\}$. We then have for $v \in V$
$$g \cdot g_i \otimes v = g g_i \otimes v = g_j h \otimes v = g_j \otimes \rho(h)(v).$$
Thus, the action of g can be imagined as a block matrix of size $d \times d$, where the $(i, j(g,i))$-block is the matrix $\rho(h(g,i))$.

Only the blocks on the diagonal contribute to the trace, and we get a diagonal block at the place i precisely when
$$g g_i = g_i h(g,i),$$
and then $h(g,i) = g_i^{-1} g g_i$. The corresponding block is then $\rho(g_i^{-1} g g_i)$ that has trace $\chi(g_i^{-1} g g_i)$. (N.B., we cannot say $\chi(g_i^{-1} g g_i) = \chi(g)$ as $g_i \notin H$ in general.) To sum up this discussion, we

have proven the important formula:

$$\mathrm{Ind}_H^G \chi(g) = \sum_{\{i: g_i^{-1} g g_i \in H\}} \chi(g_i^{-1} g g_i).$$

Note, however that changing g_i to $g_i h$ for $h \in H$ doesn't change the condition $g_i^{-1} g g_i \in H$ nor the value $\chi(g_i^{-1} g g_i)$. Thus,

Theorem 4.2.1. *The induced character is given by the formula*

$$\mathrm{Ind}_H^G \chi(g) = \frac{1}{|H|} \sum_{\{b \in G: b^{-1} g b \in H\}} \chi(b^{-1} g b). \tag{1}$$

A common notation is to write

$$\dot{\chi}$$

for the extension by zero of the character χ to G. Namely, $\dot{\chi}(x) = \chi(x)$ if $x \in H$ and 0 otherwise. We can then write the character of the induced representation as

$$\mathrm{Ind}_H^G \chi(g) = \frac{1}{|H|} \sum_{b \in G} \dot{\chi}(b^{-1} g b). \tag{2}$$

Corollary 4.2.2. *Suppose that $H \lhd G$ then $b^{-1} g b \in H$ iff $g \in H$ and so we find*

$$\mathrm{Ind}_H^G \chi(g) = \begin{cases} 0 & g \notin H \\ \frac{1}{|H|} \sum_{b \in G} \chi(b^{-1} g b) & g \in H. \end{cases}$$

Example 4.2.3. From the formula we find that the character χ^{reg} of the regular representation $\mathrm{Ind}_{\{1\}}^G \mathbb{C}$ satisfies $\chi^{reg}(g) = 0$ if $g \neq 1$ and $\chi^{reg}(1) = |G|$. It is of course easy to deduce that from the definition of the representation itself.

Example 4.2.4. Let $\zeta_1 = 1, \zeta_2 = e^{2\pi i/3}, \zeta_3 = e^{4\pi i/3}$. The three 1-dimensional representations ρ_i of A_3 are determined by

$$\rho_i((123)) = \zeta_i.$$

Let $\chi_i = \mathrm{Ind}_{A_3}^{S_3} \rho_i$. The following table gives the values of these characters on the three conjugacy classes of S_3.

	1	(12)	(123)
χ_1	2	0	2
χ_2	2	0	-1
χ_3	2	0	-1

As we shall see later, representations with the same characters are isomorphic. Therefore, we find here an example of two non-isomorphic representations of a subgroup, that is ρ_2, ρ_3, whose induced representations are isomorphic.

5. The fundamental theorems

5.1. **Decomposition into irreducible representations.** We show that every representation decomposes as a sum of irreducible representations. This establishes the irreducible representations as the fundamental building blocks of representations. Many of the theorems we will study are concerned with classifying the irreducible representations and with understanding the precise way a representation is built from irreducible representations.

To proceed, we need a lemma:

Lemma 5.1.1. *Let (ρ, V) be a representation of G. There is an inner product $\langle \cdot, \cdot \rangle$ on V that is G-invariant. That is, for all $v, w \in V$ and $g \in G$ one has*

$$\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle.$$

Proof. Let (v, w) be any inner product on V. Define

$$\langle v, w \rangle = \frac{1}{|G|} \sum_{g \in G} (\rho(g)v, \rho(g)w).$$

First, this is a G-invariant function. If $h \in G$ then

$$\begin{aligned} \langle \rho(h)v, \rho(h)w \rangle &= \frac{1}{|G|} \sum_{g \in G} (\rho(g)\rho(h)v, \rho(g)\rho(h)w) \\ &= \frac{1}{|G|} \sum_{g \in G} (\rho(gh)v, \rho(gh)w) \\ &= \langle v, w \rangle, \end{aligned}$$

because when h is fixed and g varies over G the products gh are all the elements of G, each occurring once. We also have $\langle \alpha v, w \rangle = \alpha \langle v, w \rangle$ and $\langle (v + v'), w \rangle = \langle v, w \rangle + \langle v', w \rangle$. Furthermore,

$$\begin{aligned} \langle w, v \rangle &= \frac{1}{|G|} \sum_{g \in G} (\rho(g)w, \rho(g)v) \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{(\rho(g)v, \rho(g)w)} \\ &= \overline{\langle v, w \rangle}. \end{aligned}$$

Finally, for $v \neq 0$

$$\langle v, v \rangle = \frac{1}{|G|} \sum_{g \in G} (\rho(g)v, \rho(g)v),$$

and each of the summands on the right hand side is positive. Therefore,

$$\langle v, v \rangle > 0.$$

□

Theorem 5.1.2. *Any representation (ρ, V) of G is a direct sum of irreducible representations.*

Proof. We prove that by induction on $\dim(V)$. Whenever $\dim(V) = 1$, V is irreducible. Whenever V is irreducible (of any dimension) the statement is clear.

Let V be any representation and suppose that V is reducible. Let U be a non-zero subrepresentation and let $\langle \cdot, \cdot \rangle$ be a G-invariant inner product. Then,

$$U^{\perp} = \{v \in V : \langle u, v \rangle = 0, \forall u \in U\}$$

is a sub vector space and

$$V = U \oplus U^{\perp}.$$

It remains to check that $U^{\perp}$ is a sub representation as well. Let $g \in G$ and $w \in U^{\perp}$. Then, for all $u \in U$,

$$\langle u, \rho(g)(w) \rangle = \langle \rho(g)^{-1}(u), w \rangle = 0,$$

because $\rho(g)^{-1}(u) \in U$ as well. This proves that $\rho(g)(w) \in U^{\perp}$. Therefore, for all $g \in G$, $\rho(g)(U^{\perp}) \subseteq U^{\perp}$. That is, $U^{\perp}$ is a sub representation.

Using induction for U and $U^{\perp}$, we can decompose each of them into a sum of irreducible representations. And so V itself is a sum of irreducible representations. □

Corollary 5.1.3. *Let $(\rho, V), (\tau, W)$ be representations of G and suppose that there is a surjective map of representations*

$$(\rho, V) \to (\tau, W).$$

That, is W is a quotient representation of V. Then W is isomorphic to a sub representation of V and vice-versa.

Proof. Indeed, let U be the kernel of $(\rho, V) \to (\tau, W)$ then U is a sub-representation and so is $U^{\perp}$. We get an induced isomorphism $U^{\perp} \to W$, showing that W is isomorphic to a sub-representation of V. The other direction is similar. □

5.2. **Schur's lemma.**

Lemma 5.2.1. *Let $(\rho, V), (\tau, W)$ be two irreducible representations of G. Then,*

$$\mathrm{Hom}_G(V, W) \cong \begin{cases} \mathbb{C}, & \rho \cong \tau; \\ \{0\}, & \textit{else}. \end{cases}$$

Proof. First note that whether V, W, are irreducible or not, if $T \in \mathrm{Hom}_G(V, W)$ then both $\mathrm{Ker}(T)$ and $\mathrm{Im}(T)$ are sub-representations of V and W, respectively.

In our situation, $\mathrm{Ker}(T)$ is either $\{0\}$ or V, so if T is not the zero map then $\mathrm{Ker}(T) = \{0\}$, and so T is injective. Then also $\mathrm{Im}(T)$ is not trivial. Thus, $\mathrm{Im}(T) = W$ and T is therefore an isomorphism.

Fix one such T and use it to identify V with W. Then, we need to show that

$$\mathrm{End}_G(V) \cong \mathbb{C}.$$

Let $S \in \mathrm{End}_G(V)$ and let λ be an eigenvalue of S and V_λ the corresponding (non-zero) eigenspace. Then, S is a subrepresentation: If $g \in G$ and $v \in V_\lambda$ then $S(\rho(g)v) = \rho(g)(Sv) = \rho(g)\lambda v = \lambda \cdot \rho(g)v$; that is, $\rho(g)v \in V_\lambda$. As V is irreducible, we must have $V_\lambda = V$. That is, $S = \lambda \cdot \mathrm{Id}$.

On the other hand, clearly every scalar matrix $\lambda \cdot \mathrm{Id}$ belongs to $\mathrm{End}_G(\rho)$. □

5.3. **Uniqueness of decompositions.** By Theorem 5.1.2, every representation (ρ, V) decomposes as a direct sum of irreducible representations. Buy collecting together isomorphic irreducible representations, we may assume that

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_s^{a_s},$$

where (ρ_i, V_i) are irreducible representations that are not isomorphic to each other. Suppose we have another such decomposition. By allowing also exponents $a_i = 0$, we may assume that the other decomposition is also written as

$$V \cong V_1^{b_1} \oplus \cdots \oplus V_s^{b_s},$$

and our claim is that $a_i = b_i$ for all i. To show that we calculate $\dim(\mathrm{Hom}_G(V_i, V))$. First, note the general fact that

$$\mathrm{Hom}(W, U \oplus V) = \mathrm{Hom}(W, U) \oplus \mathrm{Hom}(W, V),$$

and likewise

$$\mathrm{Hom}_G(W, U \oplus V) = \mathrm{Hom}_G(W, U) \oplus \mathrm{Hom}_G(W, V).$$

Therefore, by using Schur's Lemma, we conclude that

$$\mathrm{Hom}_G(V_i, V) = \oplus_{j=1}^{s} \mathrm{Hom}_G(V_i, V_j)^{a_i} = \mathrm{Hom}_G(V_i, V_i)^{a_i} = \mathbb{C}^{a_i},$$

and, in particular,

$$\dim(\mathrm{Hom}_G(V_i, V)) = \dim(\mathbb{C}^{a_i}) = a_i.$$

As the left hand side of this last equation "doesn't know" about the decomposition, it follows that $a_i = b_i$. We have proven:

Theorem 5.3.1. *Every representation of V decomposes into a direct sum of irreducible representations. The irreducible representations and the multiplicities to which they appear are determined uniquely, up to isomorphism.*

5.4. **The character of** $\mathrm{Hom}(V,W)$**.** Let now $(\rho, V), (\tau, W)$, be any two representations of G then $\mathrm{Hom}(V,W)$ is a representation of G as well. We wish to calculate its character. Our calculation method is going to be somewhat ad hoc. Later we shall discuss tensor product of representations and make the calculation more conceptual.

Let $\{e_1,\dots,e_n\}$ be a basis for V, $\{e_1^*,\dots,e_n^*\}$ the dual basis of $V^* = \mathrm{Hom}(V,\mathbb{C})$ and let $\{f_1,\dots f_m\}$ be a basis for W. It is a pleasant exercise to show that there is a canonical isomorphism

$$V^* \otimes_k W \cong \mathrm{Hom}(V,W).$$

This isomorphism has the property that for a vector $\phi \in V^*$ and $w \in W$ the tensor $\phi \otimes w$ is mapped to the linear transformation that takes a vector $v \in V$ to $\phi(v)\cdot w$. In particular, on the basis of V it has the values

$$e_i \mapsto \phi(e_i)\cdot w, \quad i = 1,\dots,n.$$

Lemma 5.4.1. *The elements $\{e_i^* \otimes f_j, i = 1,\dots,n, j = 1,\dots,m\}$, are a basis of* $\mathrm{Hom}(V,W)$*. Assume that $\rho(g^{-1}) = (g_{ij})$ and $\tau(g) = (h_{ij})$ then*

$$\sigma(g)(e_i^* \otimes f_j) = \sum_{k,\ell} a_{k\ell}(g)\cdot e_k^* \otimes f_\ell,$$

where

$$a_{k\ell}(g) = g_{ik}h_{\ell j}. \tag{3}$$

Proof. In the bases $\{e_1,\dots,e_n\}$ and $\{f_1,\dots f_m\}$, the linear map $e_k^* \otimes f_\ell$ from V to W is given by the matrix $M = (m_{ij})$ having a unique non-zero entry, which is equal to 1, appearing in the (ℓ, k) place. Thus, from the identification $\mathrm{Hom}(V,W) \cong M_{m,n}(\mathbb{C})$ coming from the choice of bases, the claim that $\{e_i^* \otimes f_j\}$ is a basis is clear.

To understand which map is $\sigma(g)(e_i^* \otimes f_j)$, we need to figure out where does e_t goes under the linear map $\sigma(g)(e_i^* \otimes f_j)$ for $t = 1,\dots,n$. By definition,

$$\begin{aligned}\sigma(g)(e_i^* \otimes f_j)(e_t) &= \tau(g)((e_i^* \otimes f_j)(\rho(g^{-1})(e_t))\\ &= \tau(g)((e_i^* \otimes f_j)(\sum_s g_{st}e_s))\\ &= \tau(g)(g_{it}f_j)\\ &= \sum_s g_{it}h_{sj}f_s.\end{aligned}$$

On the other hand, for some scalars $a_{k\ell}(g)$ we have $\sigma(g)(e_i^* \otimes f_j) = \sum_{k,\ell} a_{k\ell}(g)e_k^* \otimes f_\ell$ and so

$$\sigma(g)(e_i^* \otimes f_j)(e_t) = (\sum_{k,\ell} a_{k\ell}(g)e_k^* \otimes f_\ell)(e_t) = \sum_\ell a_{t\ell}f_\ell.$$

Comparing, we find,

$$a_{ts}(g) = g_{it}h_{sj}.$$

□

Corollary 5.4.2. *The character χ of the representation* $\mathrm{Hom}(V,W)$ *is*

$$\chi(g) = \chi_\tau(g)\cdot\overline{\chi_\rho(g)}.$$

Proof. The formula we found in Lemma 5.4.1, $a_{ts}(g) = g_{it}h_{sj}$, should really be written so as to indicate the dependence on i and j as the formula for $a_{ts}(g)$ describe the action of $\sigma(g)$ on the specific basis element $e_i^* \otimes f_j$. Thus, we should write

$$a_{ts}^{ij}(g) = g_{it}h_{sj},$$

to indicate this dependence. In this notation,

$$\mathrm{Tr}(\sigma(g)) = \sum_{ij} a_{ij}^{ij}(g) = \sum_{ij} g_{ii}h_{jj} = \chi_\tau(g) \cdot \chi_\rho(g^{-1}) = \chi_\tau(g) \cdot \overline{\chi_\rho(g)}.$$

□

5.5. **Class functions and an inner product structure.** Let G be a group. Recall that a class function on G is a function $f\colon G \to \mathbb{C}$ that is constant on conjugacy classes. That is,

$$f(x) = f(gxg^{-1}), \quad \forall x, g \in G.$$

One calls the number of conjugacy classes of G the **class number** of G. Let us denote it by $h = h(G)$. The class functions form a vector space of dimension h that we shall denote $Class(G)$. As we have seen, for every representation ρ its character χ_ρ is a class function.

We define now a structure of inner product on $Class(G)$ by

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}.$$

For example, the constant function 1, that is also the character of the trivial one-dimensional representation of G, is a class function and its norm $\|1\| = 1$ (which explains the choice of normalization).

5.6. **The projection π.** Let (ρ, V) be a representation of G.

Lemma 5.6.1. *Let*

$$\pi = \frac{1}{|G|} \sum_{g \in G} \rho(g).$$

Then $\pi \in \mathrm{End}_G(V)$ and is a projection onto the subspace V^G.

Proof. As π is a sum of linear maps, it is a linear map itself. If $h \in G$ then

$$\rho(h) \circ \pi = \frac{1}{|G|} \sum_{g \in G} \rho(hg) = (\frac{1}{|G|} \sum_{g \in G} \rho(hgh^{-1}))\rho(h) = \pi \circ \rho(h),$$

because as g ranges over G and h is fixed, also hgh^{-1} ranges over G.

The image of π is fixed by G: let $v \in V$ then

$$\rho(h)(\pi(v)) = (\frac{1}{|G|} \sum_{g \in G} \rho(hg))(v) = (\frac{1}{|G|} \sum_{g \in G} \rho(g))(v) = \pi(v),$$

where we have used that as g ranges over G so does hg.

Finally, if $v \in V^G$ then $\pi(v) = \frac{1}{|G|} \sum_{g \in G} \rho(g)(v) = \frac{1}{|G|} \sum_{g \in G} v = v$. □

Corollary 5.6.2. *Let (ρ, V) be a representation of G and let χ_1 be the character of the trivial one dimensional representation $(\rho_1, \mathbb{C})$ of G. Consider the decomposition of ρ into irreducible representations*

$$\rho = \rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t},$$

where the a_i are positive, except a_1 which is allowed to be zero and (ρ_i, V_i) are non-isomorphic and irreducible. Then

$$V^G = V_1^{a_1}$$

and

$$a_1 = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g) = \langle \chi_\rho, \chi_1\rangle,$$

where $\chi_1 = \chi_{\rho_1}$ *is the constant function* 1.

Proof. We have $V^G = \oplus_i (V_i^{a_i})^G = \oplus (V_i^G)^{a_i}$. But for $i \neq 1$, V_i is irreducible and non-trivial and so $V_i^G = \{0\}$. It follows that $V^G = V_1^{a_1}$.

Now, the projection operator $\pi \in \mathrm{Hom}_G(V,V)$ and in the decomposition above

$$\pi = id_{a_1} \oplus 0 \oplus \cdots \oplus 0.$$

Therefore, $a_1 = \mathrm{Tr}(\pi) = \mathrm{Tr}(\frac{1}{|G|}\sum_{g\in G}\rho(g)) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(\rho(g)) = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g) = \langle\chi_\rho,\chi_1\rangle$. □

5.7. **Irreducible characters are orthonormal functions.** Let $(\rho, V), (\tau, W)$, be irreducible representations. We apply the considerations of Corollary 5.6.2 to the representation $\mathrm{Hom}(V,W)$. Recall that its invariants are $\mathrm{Hom}(V,W)^G = \mathrm{Hom}_G(V,W)$. On the one hand, by Schur's Lemma, the dimension of $\mathrm{Hom}_G(V,W)$ is 0 if $\rho \not\cong \tau$ and 1 if $\rho \cong \tau$. On the other hand, by Corollary 5.4.2 and Corollary 5.6.2,

$$\dim\ \mathrm{Hom}(V,W)^G = \frac{1}{|G|}\sum_{g\in G}\bar{\chi}_\rho(g)\chi_\tau(g) = \langle\chi_\tau,\chi_\rho\rangle.$$

Therefore, we have obtained

Theorem 5.7.1. *Let* ρ, τ *be irreducible representations of G. Then*

$$\langle\chi_\rho,\chi_\tau\rangle = \begin{cases} 1, & \text{if } \rho\cong\tau, \\ 0, & \text{if } \rho\not\cong\tau. \end{cases}$$

We arrive the following remarkable result.

Corollary 5.7.2. *The characters of the irreducible representations of G form an orthonormal set in* $Class(G)$. *In particular, there are finitely many irreducible representations up to isomorphism, in fact at most* $\dim\ Class(G) = h(G)$.

We shall shortly see that there are precisely that many isomorphism classes of irreducible representations and so their characters are an orthonormal *basis* of $Class(G)$.

Corollary 5.7.3. *The character of a representation determines it up to isomorphism.*

Proof. Indeed, if

$$\rho \cong \oplus_i \rho_i^{a_i},$$

where the ρ_i are non-isomorphic irreducible representations then $\chi_\rho = \sum a_i\chi_{\rho_i}$ and by orthogonality we find

$$a_i = \langle\chi_\rho,\chi_{\rho_i}\rangle.$$

In addition, as the χ_{ρ_i} are linearly independent, the expression $\chi_\rho = \sum a_i\chi_i$ is unique. □

Corollary 5.7.4. *A representation* ρ *is irreducible if and only if* $\|\chi_\rho\| = 1$.

Proof. Indeed, if $\chi_\rho = \sum_{i=1}^d a_i\chi_{\rho_i}$, where the ρ_i are irreducible and distinct then $\|\chi_\rho\| = \sum_{i=1}^d a_i^2$. This sum is equal to 1 if and only if there is a unique a_i that is 1 and all the rest are zero. That is, if and only if ρ is irreducible. □

Corollary 5.7.5. *Let ρ be a representation and consider its decomposition into irreducible representations*

$$\rho \cong \rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t}.$$

Then

$$a_i = \langle \chi_\rho, \chi_{\rho_i} \rangle.$$

Proof. This was proven in the course of proving Corollary 5.7.3. □

5.8. **Further study of the regular representation.** Recall the regular representation ρ^{reg} of G from § 3.4.3.

Theorem 5.8.1. *Any irreducible representation ρ appears in ρ^{reg}. In fact, it appears in multiplicity equal to its dimension. In particular, if $\rho_1, \dots, \rho_t$ are the irreducible representations of G then*

$$|G| = \sum_{i=1} \dim(\rho_i)^2.$$

Proof. We need to show that $\langle \rho, \rho^{reg} \rangle \neq 0$. But

$$\langle \rho, \rho^{reg} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \bar{\chi}_{reg}(g) = \chi_\rho(1) = \dim\ \rho.$$

From this the statement $\rho^{reg} = \sum_{i=1}^t \dim \rho_i \cdot \chi_{\rho_i}$ follows. The last statement is obtained by considering the dimensions of the representation spaces on both sides. □

Lemma 5.8.2. *Let $\alpha \in Class(G)$. For any representation (ρ, V),*

$$\sum_{g \in G} \alpha(g) \cdot \rho(g) \in \mathrm{End}_G(V).$$

Proof. As a sum of linear maps, certainly $\sum_{g \in G} \alpha(g) \cdot \rho(g) \in \mathrm{End}(V)$. We only need to check that it commutes with the group action. Now, using that ρ is a homomorphism, for $h \in G$ we have

$$\begin{aligned} \rho(h) \circ (\sum_{g \in G} \alpha(g) \cdot \rho(g)) &= \sum_{g \in G} \alpha(g) \cdot \rho(hgh^{-1}) \rho(h) \\ &= (\sum_{g \in G} \alpha(hgh^{-1}) \cdot \rho(hgh^{-1})) \rho(h) \\ &= (\sum_{g \in G} \alpha(g) \cdot \rho(g)) \circ \rho(h), \end{aligned}$$

because $\alpha(g) = \alpha(hgh^{-1})$ for all g and h. □

Theorem 5.8.3. *The number of irreducible representations of G is its class number $h(G)$ and the characters of the irreducible representations form an orthonormal basis for $Class(G)$.*

Proof. We know that the characters of the irreducible representations are an orthonormal set in $Class(G)$. If they are not a basis, there is some function $\beta \in Class(G)$ that is orthogonal to all these characters. Let α be the function $\alpha(g) = \overline{\beta(g)}$; note that also $\alpha \in Class(G)$. We will show that $\alpha \equiv 0$ (namely, α is the zero function), thus $\beta \equiv 0$, and so the characters of irreducible representations are a basis for $Class(G)$. Consequently, their number is the class number of G.

Let (ρ, V) be an irreducible representations of G of dimension d. We claim that the operator $A_\rho = \sum_{g \in G} \alpha(g) \cdot \rho(g)$ is the zero operator

$$A_\rho \colon V \to V.$$

Indeed, as $\mathrm{End}_G(V) = \mathbb{C}$, where the isomorphism is given by $T \mapsto \frac{1}{d}\mathrm{Tr}(T)$, since $A_\rho \in \mathrm{End}_G((\rho, V))$ by Lemma 5.8.2, we can determine it by $\frac{1}{d}\mathrm{Tr}(A_\rho)$. Let us calculate:

$$\frac{1}{d}\mathrm{Tr}(A_\rho) = \frac{1}{d}\sum_{g \in G} \alpha(g) \cdot \chi_\rho(g) = \langle \chi_\rho, \beta \rangle = 0.$$

It follows that A_ρ is zero.

Now, this holds for any irreducible representation V and, therefore, for any sum of irreducible representations. In particular, it holds for the regular representation $\mathbb{C}[G]$ of G. (Note that for $\rho \oplus \tau$ we have naturally, $A_{\rho\oplus\tau} = A_\rho \oplus A_\tau$, etc.) The last step in the proof is to realize that the linear operators $\rho^{reg}(g) \in \mathrm{Aut}(\mathbb{C}[G])$ are linearly independent and thus, $A_{\rho^{reg}} = 0$ implies that $\alpha \equiv 0$.

Suppose a linear dependence between the operators $\{\rho^{reg}(g)\}$; namely, suppose that we have $\sum_g \gamma(g)\rho^{reg}(g) = 0$ for some scalars $\gamma(g) \in \mathbb{C}$. Apply this operator to the vector $[e] \in \mathbb{C}[G]$ (where e is the identity element of G). Then

$$\sum_g \gamma(g)\rho^{reg}(g)([e]) = \sum_g \gamma(g)[g] = 0.$$

As $\{[g] : g \in G\}$ are a basis for $\mathbb{C}[G]$, we conclude that all $\gamma(g) = 0$. □

A very useful fact that we will not prove (as it requires techniques from number theory) is the following.

Fact. *Let ρ be an irreducible representation of a group G then*

$$\dim(\rho) | \sharp\, G.$$

5.9. **Frobenius reciprocity.**

As we shall see later, Frobenius reciprocity in its precise form is a very useful tool to analyze induced representations. The importance of this rests on the fact that induced representations are a very powerful method to arrive at the irreducible representations of a group G starting from its subgroups. We have already seen a form of Frobenius reciprocity in § 2.7.

Given a group G we denote $\langle \alpha, \beta \rangle_G$ the inner product of its characters.

Theorem 5.9.1. *Let H be a subgroup of a finite group G and let V be a representation of H with character ρ and W a representation of G with character σ. Then*

$$\langle \mathrm{Ind}_H^G \rho, \sigma \rangle_G = \langle \rho, \mathrm{Res}_H^G \sigma \rangle_H.$$

We note an immediate conclusion: if ρ and σ are irreducible representations of H and G, respectively, then the multiplicity to which σ appears in the induced representation $\mathrm{Ind}_H^G \rho$ is equal to the multiplicity to which ρ appears in σ restricted to the subgroup H.

Proof. We'll just calculate!

$$\begin{aligned}
\langle \mathrm{Ind}_H^G \rho, \sigma \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \mathrm{Ind}_H^G \rho(g) \cdot \overline{\sigma(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} \left(\frac{1}{|H|} \sum_{h \in G} \dot{\rho}(h^{-1}gh) \right) \cdot \overline{\sigma(g)} \\
&= \frac{1}{|H| \cdot |G|} \sum_{t \in H} \sum_{\{g, h \in G, h^{-1}gh = t\}} \rho(t) \cdot \overline{\sigma(hth^{-1})} \\
&= \frac{1}{|H|} \sum_{t \in H} \rho(t) \cdot \overline{\sigma(t)} \\
&= \langle \rho, \sigma \rangle_H.
\end{aligned}$$

We used the fact in $\{g, h \in G, h^{-1}gh = t\}$, actually $g = hth^{-1}$ and so is uniquely determined by h that can be arbitrary, and that for $h, t \in G$ we have $\sigma(hth^{-1}) = \sigma(t)$ because σ is a representation of G. □

Applying Frobenius reciprocity, one may deduce the following (details left as exercise).

Corollary 5.9.2. *Let $H \lhd G$ and let (σ, W) be an irreducible representation of H. Then $\mathrm{Ind}_H^G \sigma$ is irreducible if and only if for all $g \in G \setminus H$ the representation*

$$\sigma^g : H \to \mathrm{GL}(W), \quad \sigma^g(h) = \sigma(g^{-1}hg),$$

is not isomorphic to σ. In particular, we must have $\mathrm{Cent}_G(H) \subseteq H$.

5.10. **Blichfeldt's theorem.** Blichfeldt's theorem is a rather striking result that asserts that for supersolvable groups, in particular, for p-groups, every irreducible representation is induced from a 1-dimensional representation of a subgroup.

5.10.1. *Supersolvable group.* Let G be a finite group. We say that G is **supersolvable** if there is a sequenece of subgroups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_N = \{1\}, \tag{4}$$

of subgroups G_i, such that each G_i is a normal subgroup of G (not just of G_{i-1}!) and such that G_{i-1}/G_i is cyclic for $i = 1, \dots, N$. We have proven that every p-group is supersolvable (without using this terminology) in MATH 456.

It is a standard argument to show that subgroups and quotient groups of supersolvable groups are supersolvable. However, it is not true that an extension of a supersolvable group by a supersolvable group is supersolvable. For example, the group S_4 sits in an exact sequence $1 \to V \to S_4 \to S_3 \to 1$, where V and S_3 are supersolvable, but S_4 is not supersolvable; S_4 doesn't have any normal subgroup of order 2 or 3. We see that

$$\text{supersolvable} \underset{\not\Longleftarrow}{\Longrightarrow} \text{solvable}.$$

However, a direct product of supersolvable groups is supersolvable.

Theorem 5.10.1 (Blichfeldt)**.** *Let G be a supersolvable group and let ρ be an irreducible representation of G then*

$$\rho \cong \mathrm{Ind}_J^G \psi,$$

where J is a subgroup of G and ψ a 1-dimensional representation of it.

Proof. The proof is a mix of induction on the order of G and another reduction to the faithful case. The base of the induction is the case where G is cyclic of prime order in which case any irreducible representation is one dimensional and so we may take $J = G$.

Now for the general case: we first assume that G acts faithfully. Namely, that

$$\rho : G \to \mathrm{GL}(V),$$

is an injective map.

First note that if G is abelian there is nothing to prove; ρ must be one dimensional and we take $J = G$.

Lemma 5.10.2. *Let G be a non-abelian supersolvable group. Then G has an abelian normal subgroup N such that $N \not\subseteq Z(G)$.*

Proof. (Lemma) Let G_i be the minimal subgroup in (4) such that $G_i \not\subseteq Z(G)$. Then $G_{i+1} \subseteq Z(G)$ and G_i/G_{i+1} is cyclic. From an exercise of MATH 456 the group G_i is then abelian. □

Fix this subgroup N and consider V as a representation of N. As N is abelian, V decomposes as a direct sum over the character group of N:

$$V = \oplus_{\psi \in \hat{N}} V_\psi,$$

where $V_\psi = \{v \in V : \rho(n)v = \psi(n)v, \forall n \in N\}$. Pick a ψ such that $V_\psi \neq \{0\}$. For $g \in G$ let

$$\psi^g \colon N \to \mathbb{C}^\times, \qquad \psi^g(n) = \psi(g^{-1}ng).$$

These are characters of G. Let $S = \{\psi^g : g \in G\} \subseteq \hat{N}$. Let $H = \{g \in G : \psi^g = \psi\}$. Then,

$$\sharp S = [G : H].$$

Now, it is easy to check that

$$\rho(g)(V_\chi) = V_{\chi^g}.$$

Thus, in fact,

$$V = \oplus_{\chi \in S} V_\chi.$$

Note that for every $\chi \in S$ we have an isomorphism of vector spaces $V_\chi \cong V_\psi$ (but not as representations) and that give

$$\dim(V) = \sharp S \cdot \dim(V_\psi).$$

Now consider the map of representations, given on pure tensors by $g \otimes v \mapsto \rho(g)(v)$,

$$\mathrm{Ind}_H^G V_\psi = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V_\psi \to V. \tag{5}$$

As this is not the zero map and V is irreducible, this map is surjective. The dimension of the l.h.s is $[G : H] \cdot \dim(V_\psi) = \sharp S \cdot \dim(V_\psi) = \dim(V)$ and therefore the map is an isomorphism.

In fact, we claim that S has more than one element (and consequently H is a proper subgroup of G). Indeed, if S has only one element then $\psi^g = \psi$ for all $g \in G$ and $V = V_\psi$. That is, for all $n \in N$ and $g \in G$ we have

$$\rho(g^{-1}ngn^{-1}) = \psi(g^{-1}ngn^{-1}) = 1.$$

As G is faithful, this implies that $g^{-1}ngn^{-1} = 1$ for all $n \in N, g \in G$. But that implies $N \subseteq Z(G)$. Contradiction!

Thus, we have proven that $V \cong \mathrm{Ind}_H^G V_\psi$ for some proper subgroup H of G. Note that V_ψ is an irreducible representation of H, else the isomorphism in (5) would imply that V is reducible too. As H is a supersolvable subgroup of smaller order, we may apply the induction hypothesis to conclude that

$$V_\psi \cong \mathrm{Ind}_J^H U,$$

where U is a 1-dimensional representation of a subgroup J of H. Then

$$V \cong \mathrm{Ind}_H^G \mathrm{Ind}_J^H U \cong \mathrm{Ind}_J^G U,$$

and the proof is complete for the case where G acts faithfully.

Suppose that G doesn't act faithfully and let $G_0 = \mathrm{Ker}(\rho)$. Using the first isomorphism theorem, there is an injective homomorphism $\rho_0\colon G/G_0 \to GL(V)$ such that ρ is the composition $G \to G/G_0 \overset{\rho_0}{\to} \mathrm{GL}(V)$. As G/G_0 is a supersolvable group of smaller order, we can apply induction and conclude that

$$\rho_0 \cong \mathrm{Ind}_{J'}^{G/G_0} U,$$

for some one dimensional representation U of a subgroup J' of G/G_0 (where we view both sides also as representations of G). Let J be the preimage of J' under the homomorphism $G \to G/G_0$. Then, viewing U as a 1-dimensional representation of J, one finds, for example by calculating characters,

$$\rho \cong \mathrm{Ind}_J^G U.$$

□

Example 5.10.3. Let G be the subgroup of $\mathrm{GL}_3(\mathbb{F}_p)$ consisting of the matrices $\begin{pmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{pmatrix}$. One check that $Z(G) = G'$ and equal to the matrices $\begin{pmatrix} 1 & 0 & * \\ & 1 & 0 \\ & & 1 \end{pmatrix}$. As $G/G' \cong \mathbb{F}_p \oplus \mathbb{F}_p$, the group G has p^2 1-dimensional representations (and using this isomorphism it is easy to establish that G is supersolvable). As $p^3 = |G|$ is the sum of the squares of the dimensions of the irreducible representations, G cannot have an irreducible representation of dimension p^2. Note that every irreducible representation of G that is not 1-dimensional is a faithful representation of G (because, else, it will come from a non-trivial quotient of G but those are all abelian – being p groups of order at most p^2 – and all their irreducible representations are 1-dimensional). We deduce, therefore, from Blichfeldt's theorem, or rather from its proof, that taking $N = \begin{pmatrix} 1 & * & * \\ & 1 & 0 \\ & & 1 \end{pmatrix}$, every irreducible representation of G that is not 1-dimensional is p-dimensional and isomorphic to $\mathrm{Ind}_N^G \psi$ where ψ is a 1-dimensional character of N.

Now, the group N is isomorphic to $\mathbb{F}_p^2$ and it has p^2 such characters. Also, examining the proof of the Blichfeldt's theorem, we see that every irreducible representation of G of the form $\mathrm{Ind}_N^G \psi$ is also of the form $\mathrm{Ind}_N^G \psi'$, for p different ψ', arising as $\psi' = \psi^g$ for some $g \in G$. Thus, the characters of N that induce irreducible representations are divided into sets S of p-elements each, and every character in S gives the same induced representation. On the other hand, by counting, we see that there must be $p-1$ irreducible representations of G of dimension p ($p^3 = p^2 \cdot 1^2 + (p-1) \cdot p^2$). This explains what happens with $p(p-1)$ characters of N. The remaining p characters induce reducible representations of G. I haven't checked, but it seems these must be the characters of the form

$$\begin{pmatrix} 1 & a & b \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mapsto \chi(b),$$

where $\chi\colon \mathbb{F}_p \to \mathbb{C}$ is a 1-dimensional character.

Remark 5.10.4. There is an important theorem, in the same circle of ideas. To state it, we will need some additional terminology. Consider the subring

$$\mathrm{ch}(\mathbb{C}[G])$$

of $\mathbb{C}[G]$ consisting of all $\mathbb{Z}$-linear combinations of the irreducible characters $\{\chi_i : i = 1, \dots, h(G)\}$. An element f of $Class(G)$ lies in $\mathrm{ch}(\mathbb{C}[G])$ if and only if $\langle f, \chi_i \rangle \in \mathbb{Z}, i = 1, \dots h(G)$. The elements of $\mathrm{ch}(\mathbb{C}[G])$ are called **virtual characters**. They are class functions f that are good candidates to be characters of representations, especially if $f(1) \geq 0$, but this condition doesn't suffice.

Let p be a prime. A group H is called **p-elementary** subgroup if H is a direct product of a p-group with a cyclic subgroup of order prime to p. It is called **elementary** if it is p-elementary for some prime p. Given a group G we can consider the family of all its elementary subgroups.

Theorem 5.10.5. **(Brauer's Induction Theorem)** *Every virtual character of G is a $\mathbb{Z}$-linear combination of characters induced from 1-dimensional characters of elementary subgroups of G. That is, any element $f \in \mathrm{ch}(\mathbb{C}[G])$ is of the form*

$$f = \sum_{H_i} a_i \cdot \mathrm{Ind}_{H_i}^{G} \psi_i,$$

for some integers a_i, elementary subgroups H_i of G and 1-dimensional characters $\psi_i \colon H_i \to \mathbb{C}^\times$.

Brauer's motivation was to prove this way that L-functions constructed in number theory have meromorphic continuation to the complex plane. This factorization formula expresses an L function associated to a Galois extension of $\mathbb{Q}$ with Galois group G as a product of Dirichlet L-functions to powers a_i. For Dirichlet L-function one knows analytic continuation and so, if one knows all the a_i are positive, one would even get holomorphic continuation, which is still an open problem known as **Artin's Conjecture**.

6. Examples

6.1. Decomposing the standard representation of S_n.

Example 6.1.1. Consider the standard representation ρ^{St} of S_n for $n \geq 2$. We saw that it decomposes as a direct sum $\mathbb{1} \oplus \rho^{St,0}$. Let χ^{St} be the character of ρ^{St} and $\chi^{St,0}$ of $\rho^{St,0}$. Then

$$\chi^{St} = \chi^{St,0} + \mathbb{1}.$$

Claim:$\|\chi^{St}\|^2 = 2$.

Proof. Let $T = \{1, \dots, n\}$. Let S_n act on $T \times T$ diagonally,

$$\sigma(a,b) = (\sigma(a), \sigma(b)).$$

It is easy to see that there are two orbits for this action: the orbit of $(1,1)$ and the orbit of $(1,2)$. Thus, by Cauchy-Frobenius formula,

$$\frac{1}{|S_n|} \sum_{\sigma \in S_n} I(\sigma) = 2.$$

Note that $I(\sigma)$, the number of fixed points of σ in its action on $T \times T$, is equal to the square of the number of fixed points of σ in its action on T because the fixed points of σ in its action on $T \times T$ are of the form (a,b) where both a and b are fixed points of σ in its action on T.

On the other hand, $\chi^{St}(\sigma)$ is the number of fixed points of σ in T. We find

$$\begin{aligned}
\|\chi^{St}\|^2 &= \frac{1}{|S_n|} \sum_{\sigma \in S_n} \chi(\sigma)\bar{\chi}(\sigma) \\
&= \frac{1}{|S_n|} \sum_{\sigma \in S_n} \chi(\sigma)^2 \\
&= \frac{1}{|S_n|} \sum_{\sigma \in S_n} I(\sigma) \\
&= 2
\end{aligned}$$

□

Now, using that $\chi^{St,0}$ and $\mathbb{1}$ are real valued, we find

$$\|\chi^{St}\|^2 = \|\mathbb{1}\|^2 + 2\langle \chi^{St,0}, \mathbb{1}\rangle + \|\chi^{St,0}\|^2.$$

Moreover, the quantity $\langle \chi^{St,0}, \mathbb{1}\rangle$ is the dimension of the invariant subspace of $\rho^{St,0}$ and so is a non-negative integer. Thus, all the numbers in the formula are non-negative integers and $\|\mathbb{1}\|^2 = 1$. It follows that $\|\chi_0\|^2 = 1$ (and $\langle \chi_1, \chi_0\rangle = 0$). This is a another proof that $\rho^{St,0}$ is an irreducible representation.

6.2. **The case where** G **is abelian.** If G is an abelian group of order n then $n = h(G)$. As we have precisely n irreducible representations, the formula

$$|G| = \sum_{i=1}^{h} \dim(\rho_i)^2$$

shows that each irreducible representation is one-dimensional. We knew that already.

6.3. **Character tables.** In the following we will give the **character tables** of certain groups of small order. The columns will be named by representatives to the distinct conjugacy classes in the group, and the rows will be named by the various characters. The number $[x]$ appearing near a representative for a conjugacy class indicates how many elements are in that conjugacy class (which is handy when calculating inner products of characters). Note that if ρ is 1-dimensional, ρ is equal to its character χ_ρ.

As the groups $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^2$ are abelian, we have the following character tables. For typographical reasons, we use χ_1 to denote the character of the trivial representation $\mathbb{1}$.

	0 [1]	1 [1]
χ_1	1	1
χ_2	1	-1

Table 1: Character table of $\mathbb{Z}/2\mathbb{Z}$

	0 [1]	1 [1]	2 [1]
χ_1	1	1	1
χ_2	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
χ_3	1	$e^{4\pi i/3}$	$e^{2\pi i/3}$

Table 2: Character table of $\mathbb{Z}/3\mathbb{Z}$

	0 [1]	(1, 0) [1]	(0, 1) [1]	(1,1) [1]
χ_1	1	1	1	1
χ_2	1	-1	-1	1
χ_3	1	-1	1	-1
χ_4	1	1	-1	-1

Table 3: Character table of $(\mathbb{Z}/2\mathbb{Z})^2$

Remark 6.3.1. Note that the rows of character tables should be orthonormal vectors (but be careful when calculating the inner product - every entry $\chi(x)$ must be weighted by the size of the conjugacy class of x that appears as $[y]$ in the heading of the column). It is also true that the columns of the character table are orthogonal – see the Exercise 19.

Another check that could be performed is based on the following. Recall that

$$\chi_{\rho^{reg}} = \sum_{i=1}^{h} \chi_i(e) \cdot \chi_i.$$

(We are using here e to denote the identity element so as to avoid confusion when the group is abelian.) That means that if we multiply each row χ_i in the character table by $\chi_i(e)$ (which is listed in the second column – the column of the identity element) and then sum up all the rescaled rows, we should get a row vector of the form $(|G|, 0, \dots, 0)$. Sometimes we can turn that around and find a missing character. This is our next example.

6.3.1. *The character table of S_3.* Consider the group S_3. We have $S_3^{ab} \cong \mathbb{Z}/2\mathbb{Z}$ and so there are precisely two 1-dimensional representations. These are the trivial representation $\mathbb{1} = \chi_1$ and the sign representation $\chi^{\rm sgn}$. Since we have

$$6 = 1^2 + 1^2 + \text{ sum of squares},$$

where each square is at least 2^2, we conclude that there is a unique additional irreducible representation of S_3 and it is 2-dimensional. From the remark above, we can even figure out its character:

$$2\chi_3 = \chi^{reg} - \chi_1 - \chi_2.$$

We thus find the character table:

	1 [1]	(12) [3]	(123) [2]
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Table 4: Character table of S_3

Luckily, we have a model for this irreducible representation: $S_3 = D_3$ acts on the equilateral triangle in the plane with the linear tranformations; this is the representation ρ^{plane} considered previously.

$$y = (23) \leftrightarrow \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad x = (123) \leftrightarrow \left(\begin{smallmatrix} \cos(2\pi/3) & \sin(2\pi/3) \\ -\sin(2\pi/3) & \cos(2\pi/3) \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{smallmatrix}\right).$$

We easily check that the character of ρ^{plane} is χ_3.

We actually have yet another model for this representation arising from the standard representation of S_3: this model consists of the vectors in $\mathbb{C}^3$ whose coordinates sum to 0, where S_3 acts by permuting the coordinates. A basis for this 2-dimensional space is given by $u = e_1 - e_2, v = e_2 - e_3$. In this basis we have

$$y = (23) \leftrightarrow \left(\begin{smallmatrix} 1 & 0 \\ 1 & -1 \end{smallmatrix}\right), \quad x = (123) \leftrightarrow \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right).$$

We called this representation $\rho^{st,0}$.

These two representations, $\rho^{st,0}$ and ρ^{plane}, are isomorphic – we see they have the same character – but that is not immediately visible from the matrices. There "ought to be" an invertible matrix M such that conjugation by it takes the first representation to the second.

There is yet a third model for this irreducible representation and it is $\mathrm{Ind}_{A_3}^{S_3}\chi$ where χ is any of the two irreducible one-dimensional characters of A_3. Cf. Example 4.2.4.

6.3.2. *The character table of* D_4. Consider the case of $G = D_4$. The commutator subgroup is given by $\{1, x^2\}$ and $G/G' \cong (\mathbb{Z}/2\mathbb{Z})^2$. We can thus lift every one-dimensional representation ρ_i of $(\mathbb{Z}/2\mathbb{Z})^2$ to D_4 and get a one-dimensional representation

$$\rho_i' : D_4 \to (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{C}^\times.$$

This gives us the four 1-dimensional representations of D_4. Once more, by using the formula $|G| = \sum_{i=1}^h \dim(\rho_i)^2$, we find that there is a unique additional irreducible representation and it is 2-dimensional. A natural guess is the representation coming from the action on the plane:

$$y = (23) \leftrightarrow \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad x = (1234) \leftrightarrow \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right).$$

(This is the representation we have denoted ρ^{plane} previously.) From this we find the following values for its character:

	1	x	x^2	x^3	y	xy	x^2y	x^3y
χ^{plane}	2	0	-2	0	0	0	0	0

We calculate that $\|\chi^{plane}\| = 1$ and therefore this representation is irreducible (even over the complex numbers!). Thus, the character table is:

	1 [1]	x [2]	x^2 [1]	y [2]	xy [2]
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	1	-1	1	1	-1
χ_4	1	1	1	-1	-1
χ^{plane}	2	0	-2	0	0

Table 5: Character table of D_4

To illustrate how useful this information is, let us consider D_4 as a subgroup of S_4 and let

$$\rho : D_4 \to \mathrm{GL}_4(\mathbb{C}),$$

be the restriction of the standard representation of S_4 to D_4 (where $x = (1234), y = (24)$ and $xy = (12)(34)$). Recall that $\chi_{\rho^{std}}(\sigma)$ is the number of fixed points of σ. Thus, we find that

	1 [1]	x [2]	x^2 [1]	y [2]	xy [2]
χ_ρ	4	0	0	2	0

Therefore, $\langle \chi_\rho, \chi_1 \rangle = \langle \chi_\rho, \chi_3 \rangle = 1$, $\langle \chi_\rho, \chi_2 \rangle = \langle \chi_\rho, \chi_4 \rangle = 0$ and $\langle \chi_\rho, \chi^{plane} \rangle = 1$. Thus, ρ decomposes as

$$\rho = \rho_1 \oplus \rho_3 \oplus \rho^{plane}.$$

Here ρ_1 is the trivial representation and ρ_3 is the representation where x^2 and y act trivially, but x acts as multiplication by -1. Consequently, there is a coordinate system on $\mathbb{C}^4$ in which D_4 acts as follows

$$x \mapsto \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & 0 \\ & & 0 & 1 \end{pmatrix}.$$

Also visible from these calculations is that there is a unique line that is fixed by the action of D_4. Indeed, the dimension of the invariants is the multiplicity of the trivial representation which is equal to 1.

6.4. **Representations of S_4.** To begin with, the number of conjugacy classes of S_4 is $p(4) = 5$. Thus, there are 5 irreducible representations. As the commutator of S_4 is A_4, $S_4^{ab} \cong \mathbb{Z}/2\mathbb{Z}$ and thus has precisely two 1-dimensional representations that must be the trivial one χ_1 and the sign representation $\chi^{\rm sgn}$. We also know the 3-dimensional irreducible sub representation $\rho^{st,0}$ of the standard representation.

As we have

$$24 = 1^2 + 1^2 + 3^2 + x^2 + y^2,$$

we conclude that S_4 has a 2-dimensional irreducible representation ρ and an additional 3 dimensional representation τ and this list (χ_1, $\chi^{\rm sgn}$, $\rho^{st,0}$, ρ, τ) is the full list of irreducible representations of S_4.

Recall the surjective homomorphism with kernel $V = \{1, (12)(34), (13)(24), (14)(23)\}$ – the Klein group,

$$S_4 \to S_3,$$

by means of which we can pullback the irreducible 2-dimensional representation of S_3. We get a representation ρ whose character χ is

	1 [1]	(12) [6]	(123) [8]	(1234) [6]	(12)(34) [3]
χ	2	0	-1	0	2

Being a pullback of an irreducible representation, it is of course irreducible, but one can also check that $\|\chi\|^2 = 1$.

Now consider the representation $\mathrm{Hom}(\rho^{\rm sgn}, \rho^{st,0})$. Its character, by Corollary 5.4.2, is the product $\chi^{st,0} \cdot \bar{\chi}^{\rm sgn} = \chi^{st,0} \cdot \chi_{\rm sgn}$ and thus is given by

	1 [1]	(12) [6]	(123) [8]	(1234) [6]	(12)(34) [3]
$\chi^{st,0}$	3	1	0	-1	-1
$\chi^{st,0} \cdot \chi_{\rm sgn}$	3	-1	0	1	-1

One calculates that $\|\chi^{st,0} \cdot \chi_{\rm sgn}\|^2 = 1$ and so $\chi^{st,0} \cdot \chi_{\rm sgn}$ is the character of the missing irreducible representation τ. We conclude that the character table of S_4 is the following:

	1 [1]	(12) [6]	(123) [8]	(1234) [6]	(12)(34) [3]
χ_1	1	1	1	1	1
χ^{sgn}	1	-1	1	-1	1
χ	2	0	-1	0	2
$\chi^{st,0}$	3	1	0	-1	-1
χ_τ	3	-1	0	1	-1

Table 6: The character table of S_4.

6.5. **Representations of A_4.** The commutator of A_4 is V, the Klein group. As A_4/V is a group of order 3, A_4 has three 1-dimensional representations. Denote them χ_1, χ_2, χ_3. On the other hand, it has 4 conjugacy classes that are represented by $1, (12)(34), (123), (132)$. We conclude from $12 = 1^2 + 1^2 + 1^2 + x^2$ that A_4 has precisely one more irreducible representation ρ and it is

3-dimensional. A natural guess is that this representation is obtained from the action of A_4 on a tetrahedron, but here we proceed differently. We have

$$A_4 \to S_4 \to \mathrm{GL}_3(\mathbb{C}),$$

by means of $\rho^{st,0}$. We can easily calculate the character χ of this representation:

element	1 [1]	(12)(34) [3]	(123) [4]	(132) [4]
χ	3	-1	0	0

As $\|\chi\|^2 = 1$ this is an irreducible representation of A_4 too. The character table is therefore the following:

	1 [1]	(12)(34) [3]	(123) [4]	(132) [4]
χ_1	1	1	1	1
χ_2	1	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
χ_3	1	1	$e^{4\pi i/3}$	$e^{2\pi i/3}$
χ	3	-1	0	0

Table 7: The character table of A_4.

6.6. **Representations of D_n.** The commutator subgroup of D_n is $\langle x^2\rangle$ and so, if n is odd $D_n^{ab} \cong \mathbb{Z}/2\mathbb{Z}$, and if n is even $D_n^{ab} \cong (\mathbb{Z}/2\mathbb{Z})^2$. Thus D_n has two 1-dimensional representations if n is odd, and four if n is even. We also know ρ^{plane}, an irreducible 2 dimensional representation. Note though that at best the sum of the squares of these irreducible representations is 8 which is almost negligent compared to $2n$ if n is large. That is, (except for D_3 and D_4) we are missing most of the irreducible representations.

We will now construct irreducible representations of D_n as induced representations. Fix an n-th root of unity $\zeta \neq 1$ and let

$$\rho_\zeta : \langle x\rangle \to \mathbb{C}^\times$$

be the 1-dimensional character given by the homomorphism

$$\rho_\zeta(x^a) = \zeta^a.$$

As $\zeta \neq 1$ varies over all n^{th} roots of unity, we get n distinct 1-dimensional characters of $H = \langle x\rangle$.

The representation

$$\mathrm{Ind}_H^{D_n}\rho_\zeta$$

has the following description. The elements $\{1, y\}$ form a set of representatives for the cosets of H and the formulas $y \cdot y = 1 \cdot 1, x \cdot y = y \cdot x^{-1}$ allows us to calculate the action of D_n:

$$x^a \mapsto \begin{pmatrix} \zeta^a & 0 \\ 0 & \zeta^{-a} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad x^a y \mapsto \begin{pmatrix} 0 & \zeta^a \\ \zeta^{-a} & 0 \end{pmatrix}.$$

The character χ_ζ of $\mathrm{Ind}_H^{D_n}\rho_\zeta$ is given by

$$\chi_\zeta(x^a) = \zeta^a + \zeta^{-a}, \quad \chi_\zeta(x^a y) = 0.$$

We see that $\chi_\zeta = \chi_{\zeta^{-1}}$ and otherwise the characters are distinct. Therefore, for n odd, this gives us $(n-1)/2$ distinct two dimensional representations.

These induced representation are, in fact, all irreducible. This can be easily deduced from Corollary 5.9.2 as the character of H given by $t \mapsto \rho_a(y^{-1}ty)$ is the character $\rho_{-a} \neq \rho_a$ (using, again, that n is odd). In addition, still for n odd, we have two 1-dimensional representations. But, as

$$1^2 + 1^2 + \frac{n-1}{2} \cdot 2^2 = 2n,$$

we have found all the irreducible representations of D_n for n odd. Similar considerations apply for the case n even.

7. Further operations on representations

7.1. **The dual representation.** Let (ρ, V) be a representation of G. Considering $\mathbb{C}$ as a trivial representation of G, $V^* = \mathrm{Hom}(V, \mathbb{C})$ is also a representation ρ^* of G, where, as per our definitions,

$$(\rho^*(g)\phi)(v) = \phi(\rho(g^{-1})v).$$

It is called the **dual representation**.

Let us choose a basis for V, viewing thus ρ as a homomorphism $\rho \colon G \to \mathrm{GL}_n(\mathbb{C})$. As is well-known, relative to the dual basis the dual operator is representation by the transpose matrix. Thus,

$$\rho^*(g) = {}^t\rho(g)^{-1}.$$

In particular, the characters satisfy:

$$\chi_{\rho^*} = \bar{\chi}_\rho.$$

This is potentially confusing, as one often uses the notation M^* for a matrix M to mean ${}^t\bar{M}$. Then, $\rho^*(g) = {}^t\rho(g)^{-1} \neq {}^t\overline{\rho(g)}$ in general, although $\mathrm{Tr}({}^t\rho(g)^{-1}) = \mathrm{Tr}({}^t\overline{\rho(g)})$.

7.2. **Tensor products of representations.** Let $(\rho, V), (\tau, W)$ be two representations of G. Then $V \otimes_k W$ is also a representation of G,

$$g \mapsto \rho(g) \otimes \tau(g).$$

Let $\{v_1, \dots, v_n\}$ be a basis for V and $w_1, \dots, w_m$ a basis of W. Then we have a basis

$$v_1 \otimes w_1, \dots, v_n \otimes w_1, v_1 \otimes w_2, \dots, v_n \otimes w_2, \dots, v_1 \otimes w_m, \dots, v_n \otimes w_m$$

for $V \otimes W$. A calculation shows that if $\rho(g) = A = (a_{ij}), \tau(g) = B = (b_{ij})$, then $\rho(g) \otimes \tau(g)$ is given by the **Kronecker product** $A \times B$

$$A \times B = \begin{pmatrix} Ab_{11} & Ab_{12} & \cdots & Ab_{1m} \\ Ab_{21} & Ab_{22} & \cdots & Ab_{2m} \\ \vdots & & \cdots & \vdots \\ Ab_{m1} & Ab_{m2} & \cdots & Ab_{mm} \end{pmatrix}.$$

We will not need it, but it's worth knowing that if the characteristic polynomial of A is the polynomial $\prod_{i=1}^n (x - \alpha_i)$ and the characteristic polynomial of B is $\prod_{i=1}^m (x - \beta_i)$ then the characteristic polynomial of $A \times B$ is the polynomial of degree mn given by $\prod_{i,j}(x - \alpha_i\beta_j)$. A much easier fact is that

$$\mathrm{Tr}(A \times B) = \mathrm{Tr}(A) \cdot \mathrm{Tr}(B).$$

And so, letting χ_ρ denote the character of ρ, etc., we have

$$\chi_{\rho\otimes\tau} = \chi_\rho \cdot \chi_\tau.$$

As consequence we find that the character of $\mathrm{Hom}(V, W) \cong V^* \otimes W$ is

$$\chi_{\rho^*} \cdot \chi_\tau = \bar{\chi}_\rho \cdot \chi_\tau,$$

as we have previously calculated.

7.3. **Symmetric products and alternating products.** The importance of symmetric products and alternating products goes much beyond representations of groups and so it's worth to spend some time on these notions.

7.3.1. *Graded rings.* Let R be a ring. R is called a **graded ring** if R decomposes as a direct sum of abelian groups

$$R = \oplus_{n=0}^{\infty} R_n,$$

such that for all m, n,

$$R_m R_n \subseteq R_{n+m}.$$

Note that R_0 is a subring of R. A two-sided ideal $I \lhd R$ is called **graded** if

$$I = \oplus_{n=0}^{\infty} I_n, \quad I_n \subseteq R_n.$$

In this case, the quotient ring R/I is also graded as

$$R/I \cong \oplus_{n=0}^{\infty} R_n/I_n.$$

It is not hard to prove that if r_i are elements R such that each $r_i \in R_{n(i)}$ then the two sided ideal I generated by them $\langle \{r_i\} \rangle$ is a graded ideal. Sometimes we will use the notation $R = \oplus_{n=0}^{\infty} R^n$ instead of $R = \oplus_{n=0}^{\infty} R_n$.

To be precise, what we described are $\mathbb{N}$-graded rings and ideals. We will also encounter $\mathbb{Z}/2\mathbb{Z}$-graded rings in the assignment. These are ring R with a decomposition $R = R_0 \oplus R_1$ such that $R_i R_j \subset R_{i+j}$, where $i + j$ is calculated modulo 2. There is a similar notion of a graded ideal.

7.3.2. *The tensor algebra and the symmetric algebra.* Let R be a commutative ring and let V be an R-module. We define

$$T^\bullet(V) = \oplus_{n=0}^{\infty} T^n(V),$$

where

$$T^0(V) = R, \quad T^1(V) = V, \quad T^n(V) = V \otimes_R V \otimes_R \cdots \otimes_R V \ \ (n-\text{times}).$$

$T^\bullet(V)$ is a graded R-algebra: for every m and n there is a natural map [5]

$$T^m(V) \times T^n(V) \to T^{m+n}(V), \quad (v_1 \otimes \cdots \otimes v_m, w_1 \otimes \cdots \otimes w_n) \mapsto v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n.$$

This extends to define a product law on $T^\bullet(V)$, the **tensor algebra** of V.

[5] To be honest, to show that this map is well-defined requires an argument. For that we assume that $T^n(V)$ "solves" the problem of R-multiadditive, or even R-multilinear, maps $V \times \cdots \times V \to W$ for any W, much in the same way that $V \otimes V$ "solves" the problem of R-biadditive, or bilinear, maps. See also § 7.4. For fixed $(w_1, \cdots, w_n)$, the map

$$V^m \to T^{m+n}, \quad (v_1, \ldots, v_m) \mapsto v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n,$$

is an R-multilinear map. Thus, we get a well-defined homomorphism of R-modules

$$\varphi_{(w_1,\ldots,w_n)} \colon T^m \to T^{m+n}, \quad v_1 \otimes \cdots \otimes v_m \mapsto v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n.$$

This provides an R-multilinear map

$$V^n \to \mathrm{Hom}(T^m, T^{n+m}), \quad (w_1, \ldots, w_n) \mapsto \varphi_{(w_1,\ldots,w_n)},$$

and one concludes a homomorphism

$$T^n(V) \to \mathrm{Hom}_R(T^m, T^{n+m}),$$

given on pure tensors by

$$w_1 \otimes \cdots \otimes w_n \mapsto \varphi_{(w_1,\ldots,w_n)}.$$

We finally get a well-defined map

$$T^m(V) \times T^n(V) \to T^{m+n}(V),$$

given on pure tensors by

$$(v_1 \otimes \cdots \otimes v_m, w_1 \otimes \cdots \otimes w_n) \mapsto \varphi_{(w_1,\ldots,w_n)}(v_1 \otimes \cdots \otimes v_m) = v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n,$$

and the fact that it is an R-bilinear map.

Assume that V is a free R-module of rank d with a basis $e_1, \dots, e_d$, then $T^n(V)$ is a free R-module of rank d^n with the basis

$$\{e_{i_1} \otimes \cdots \otimes e_{i_n} : 1 \leq i_j \leq d\}.$$

We let I be the two-sided ideal generated by all the tensors $\{x \otimes y - y \otimes x : x, y \in V\}$ where $1 \leq i, j \leq d$. Then I is a graded ideal

$$I = \oplus_{n=0}^{\infty} I_n,$$

where, in fact $I_0 = I_1 = 0$, I_2 is the R-span of the elements $\{x \otimes y - y \otimes x : x, y \in V\}$ and I_n is the R-span of the elements

$$\{x_1 \otimes x_2 \otimes \cdots \otimes x_n - x_{\sigma(1)} \otimes x_{\sigma(2)} \otimes \cdots \otimes x_{\sigma(n)} : x_i \in V, \sigma \in S_n\}.$$

We define the **symmetric algebra**

$$\mathrm{Sym}^{\bullet}(V) = T^{\bullet}(V)/I = \oplus_{n=0}^{\infty} T^n/I_n,$$

and denote its graded pieces by

$$\mathrm{Sym}^n(V) := T^n(V)/I_n.$$

We shall denote the image of the tensor $v_1 \otimes \cdots v_n$ of $V^{\otimes n}$ in $\mathrm{Sym}^n(V)$ by $v_1 \cdots v_n$ (remembering that we are allowed now to switch the order of the v_i as we please).

Suppose that $R = \mathbb{C}$. If G acts on the finite dimensional vector space V linearly, then it acts linearly on each $T^n(V)$, and so on $T^{\bullet}(V)$, by

$$g \cdot v_1 \otimes \cdots \otimes v_n = gv_1 \otimes gv_2 \otimes \cdots \otimes gv_n.$$

The ideal I is a G-representation as well and so $\mathrm{Sym}^{\bullet}(V)$ is a graded G-representation and each graded piece is a finite dimensional representation of V. It is not hard to see that

$$\{e_{i_1} \otimes \cdots \otimes e_{i_n} : 1 \leq i_1 \leq \cdots \leq i_n \leq d\}$$

is a basis of $\mathrm{Sym}^n(V)$ and therefore

$$\dim(\mathrm{Sym}^n(V)) = \binom{n+d-1}{n}.$$

Remark 7.3.1. Choose a basis $x_1, \dots, x_d$ to V. It is not hard to see then that a basis for $V^{\otimes n}$ is

$$\{x_{i_1} x_{i_2} \cdots x_{i_n} : i_j \in \{1, \dots, d\}\}.$$

(It has cardinality d^n.) Thus, we may view $T^{\bullet}(V)$ as the ring of polynomials in the *non-commuting* variables $x_1, \dots, x_d$. To bring out this interpretation we have on purpose written $x_{i_1} x_{i_2} \cdots x_{i_n}$ instead of $x_{i_1} \otimes x_{i_2} \otimes \cdots \otimes x_{i_n}$. From this perspective, $\mathrm{Sym}^{\bullet}(V)$ can be interpreted as the ring of (usual) complex polynomials in the variables $x_1, \dots, x_n$ and a basis for $\mathrm{Sym}^n(V)$ is the given by the monomials

$$\{x_1^{i_1} \cdots x_d^{i_d} : i_j \geq 0, i_1 + \cdots + i_d = n\},$$

and has cardinality $\binom{n+d-1}{n}$.

7.3.3. *Example.* Let us deviate now from our usual conventions and allow G to be the infinite group $\mathrm{GL}_2(\mathbb{C})$. Let us take $V = \mathbb{C}^2$ the standard representation of $\mathrm{GL}_2(\mathbb{C})$, but let us think about it as linear forms $\alpha x + \beta y$, where $\alpha, \beta \in \mathbb{C}$. A matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts by sending x $(= {}^t(1,0))$ to $ax + cy$ $(= {}^t(a,b))$ and y to $bx + dy$. That is, the action amounts to linear change of variables.

In this interpretation, an element of $\mathrm{Sym}^n(V)$ is a homogeneous polynomial $f(x,y)$ of degree n and the action is

$$f(x,y) \mapsto f(ax+cy, bx+dy).$$

We get therefore a series of representations of $\mathrm{GL}_2(\mathbb{C})$, $\{\mathrm{Sym}^n(V) : n = 0,1,2,\dots\}$. There is also the series of one dimensional representations $\{\det^n : n \in \mathbb{Z}\}$. Combined, we find that representations

$$\det{}^a \otimes \mathrm{Sym}^b(V), \qquad a \in \mathbb{Z}, b \in \mathbb{N}.$$

It turns out that all these representations are irreducible and non-isomorphic. Furthermore, every *algebraic* representation of $\mathrm{GL}_2(\mathbb{C})$, i.e., every homomorphism of groups $\mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ given by rational functions $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (f_{ij}(a,b,c,d))$, where the f_{ij} are of the form of a polynomial in a,b,c,d divided by some power of the determinant, is one of these representations. This gives a complete classification of the representations of $\mathrm{GL}_2(\mathbb{C})$. A similar theory exists for any algebraic group, or even Lie group, in place of $\mathrm{GL}_2(\mathbb{C})$.

7.3.4. *The character of* Sym^2. Suppose that G acts on V with character χ. The character of the representation $T^2(V)$ is therefore χ^2. To calculate the character of $\mathrm{Sym}^2(V)$ take an element $g \in G$ and a basis $\{e_1, \dots, e_d\}$ for V on which it acts diagonally, say by $\mathrm{diag}(\alpha_1, \dots, \alpha_d)$. It acts then on e_ie_j by $\alpha_i\alpha_j$ and so we find that the trace is $\sum_{i \leq j} \alpha_i\alpha_j$. We arrive at the following formula

$$\chi_{\mathrm{Sym}^2(V)}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)). \tag{6}$$

Let us look at an example. Recall the character table of S_4.

	1 [1]	(12) [6]	(123) [8]	(1234) [6]	(12)(34) [3]
χ_1	1	1	1	1	1
χ^{sgn}	1	-1	1	-1	1
χ	2	0	-1	0	2
$\chi^{st,0}$	3	1	0	-1	-1
χ_τ	3	-1	0	1	-1

$\mathrm{Sym}^2(\chi)$ is the character of a 3-dimensional representation and is calculated as follows:

	1 [1]	(12) [6]	(123) [8]	(1234) [6]	(12)(34) [3]
χ	2	0	-1	0	2
χ^2	4	0	1	0	4
$\chi(g^2)$	2	2	-1	2	2
$\mathrm{Sym}^2(\chi)$	3	1	0	1	3

Using characters we find that $\mathrm{Sym}^2(\chi)$ is reducible and in fact

$$\mathrm{Sym}^2(\chi) = \chi_1 + \chi.$$

7.3.5. *The exterior algebra.* The exterior algebra is likewise constructed as a quotient of the tensor algebra by a graded ideal $J = \oplus_{n=0}^{\infty} J_n$. But now we want tensors to anti-commute. Thus, we want that under the map

$$T^n \rightarrow \bigwedge^n V := V^{\otimes n}/J_n,$$

that the image of $v_1 \otimes \cdots v_n$ is equal to the image of $\mathrm{sgn}(\sigma) v_{\sigma(1)} \otimes \cdots v_{\sigma(n)}$. It turns out that a better condition is to require that if in $v_1 \otimes \cdots v_n$ we have $v_i = v_j$ for some $i < j$ then its image in $\bigwedge^n(V)$ is zero. This implies the previous relation, but is a strictly stronger condition if $1 = -1$ in R. Thus, we define

$$J_n = \mathrm{Span}_R\{v_1 \otimes \cdots \otimes v_n : v_i \in V, \exists i < j \text{ s.t. } v_i = v_j\}.$$

Then $J = \oplus_{n=0}^{\infty} J_n$ is a graded two-sided ideal and we define the **exterior algebra**

$$\bigwedge^\bullet V = T^\bullet(V)/J;$$

It is an R-algebra. We denote the image of $v_1 \otimes \cdots \otimes v_n$ in $\bigwedge^\bullet V$ by

$$v_1 \wedge \cdots \wedge v_n.$$

If $R = k$ is a field, $e_1, \dots e_d$ is a basis for V, we can calculate that

$$\{e_{i_1} \wedge \cdots \wedge e_{i_n} : 1 \leq i_1 < \cdots < i_n \leq d\}$$

is a basis for $\bigwedge^n V$ and so

$$\dim_k(\bigwedge^n V) = \binom{d}{n}.$$

To be honest, this is not obvious; see Exercise 8 for details. Some notable special cases are

$$\bigwedge^0 V = k, \quad \bigwedge^1 V = V, \quad \bigwedge^d V \cong k, \quad \bigwedge^n V = \{0\} \ \ \forall n > d.$$

Example 7.3.2. Decomposition of $V^{\otimes 2}$. Assume that V is a vector space over $\mathbb{C}$. The surjections

$$V \otimes V \rightarrow \mathrm{Sym}^2(V), \qquad V \otimes V \rightarrow \bigwedge^2 V,$$

have sections. For the image of the first section, we can take the subspace spanned by the vectors $\{\frac{1}{2}(e_i \otimes e_j + e_j \otimes e_i) : 1 \leq i \leq j \leq d\}$, of dimension $d(d+1)/2$, and for the other the subspace spanned by $\{\frac{1}{2}(e_i \otimes e_j - e_j \otimes e_i) : 1 \leq i < j \leq d\}$ of dimension $d(d-1)/2$. Abusing notation, we denote them also

$$\mathrm{Sym}^2(V) \subset V, \qquad \bigwedge^2 V \subset V.$$

Note that $\bigwedge^2 V$ maps to zero on the projection $V \otimes V \rightarrow \mathrm{Sym}^2(V)$ and so we find that the two spaces are complementary and, by dimension count,

$$V \otimes V = \mathrm{Sym}^2(V) \oplus \bigwedge^2 V.$$

Passing to characters, and making use of Equation (6), we find the identity

$$\chi_V(g)^2 = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)) + \frac{1}{2}(\chi_V(g)^2 - \chi_v(g^2)),$$

where χ_V is the character of the representation V.

Example 7.3.3. Let $\rho^{St,0}$ be the irreducible representation of dimension $n-1$ of S_n contained in its standard representation ρ^{St}. We claim that $\bigwedge^a \rho^{St,0}$ is irreducible as well for all $1 \leq a \leq n-1$. We follow Fulton-Harris.

Lemma 7.3.4. *Let χ be the character of $\bigwedge^a \rho^{St}$ of S_n, for some $1 \leq a \leq n-1$. Then*

$$\|\chi\|^2 = 2.$$

Proof. Choose a basis $e_1, \dots, e_n$ for ρ^{St}. Note that there is a bijection between subsets $B \subseteq \{1, 2, \dots, n\}$ of a elements and basis elements of $\bigwedge^a \rho^{St}$; to $B = \{i_1 < \cdots < i_a\}$ is associated the basis element $e_{i_1} \wedge \cdots \wedge e_{i_a}$. Define for $\sigma \in S_n$ and such a subset B,

$$\sigma\{B\} = \begin{cases} 0 & \sigma(B) \neq B, \\ 1 & \sigma(B) = B,\ \sigma|_B \text{ is even}, \\ -1 & \sigma(B) = B,\ \sigma|_B \text{ is odd}. \end{cases}$$

The point of this definition is that

$$\chi(\sigma) = \sum_B \sigma\{B\}.$$

As this is a sum of integers

$$\bar{\chi}(\sigma) = \chi(\sigma).$$

Therefore,

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{n!} \sum_{\sigma \in S_n} \Big(\sum_{|B|=a} \sigma\{B\} \Big)^2 \\ &= \frac{1}{n!} \sum_{\sigma \in S_n} \sum_{|B|=a} \sum_{|C|=a} \sigma\{B\} \cdot \sigma\{C\} \\ &= \frac{1}{n!} \sum_{|B|=a} \sum_{|C|=a} \sum_{\substack{\sigma \in S_n \\ \sigma(B)=B \\ \sigma(C)=C}} \sigma\{B\} \cdot \sigma\{C\}. \end{aligned}$$

Now, any permutation σ such that $\sigma(B) = B$ and $\sigma(C) = C$ can be written as product,

$$\sigma = \sigma_1 \sigma_2 \sigma_3 \sigma_4,$$

where,

$$\sigma_1 \in S_{\{1,\dots,n\}-\{B \cup C\}}, \quad \sigma_2 \in S_{B-C}, \quad \sigma_3 \in S_{C-B}, \quad \sigma_4 \in S_{B \cap C}.$$

Let also $\ell = \ell_{B,C} := \sharp B \cap C$. Below, we should note that the argument also works for $\ell = a$ under the conventions $S_\emptyset = \{1\}$ and $\mathrm{sgn}(1) = 1$. Then, continuing our calculation, we find that

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{n!} \sum_{|B|=a} \sum_{|C|=a} \sum_{\sigma_1 \in S_{n-(2a-\ell)}} \sum_{\sigma_2 \in S_{a-\ell}} \sum_{\sigma_3 \in S_{a-\ell}} \sum_{\sigma_4 \in S_\ell} \mathrm{sgn}(\sigma_4)^2 \, \mathrm{sgn}(\sigma_2) \, \mathrm{sgn}(\sigma_3) \\ &= \frac{1}{n!} \sum_{|B|=a} \sum_{|C|=a} (n-(2a-\ell))! \cdot \ell! \times \Big(\sum_{\sigma_2 \in S_{a-\ell}} \mathrm{sgn}(\sigma_2) \Big)^2 \end{aligned}$$

In the calculation above we should note that ℓ is really $\ell_{B,C}$, i.e. it depends on B and C, but we omitted that from the notation which is quite cumbersome as it is. But, we should note now that if $a - \ell > 1$ then $\sum_{\sigma_2 \in S_{a-\ell}} \mathrm{sgn}(\sigma_2) = 0$ as this sum is $n! \cdot \langle \chi_{\mathrm{sgn}}, \mathbb{1} \rangle = 0$ for the sign representation and the trivial representation $\mathbb{1}$ of $S_{a-\ell}$. To continue the calculation we consider separately the case $\ell = a$ where $B = C$ and the case $\ell = a - 1$ where $B \cap C$ has $a - 1$ elements. We find, using that $\binom{n}{a}$ is the number of choices of B,

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{n!} \left(\sum_{|B|=a} (n-a)!a! + \sum_{|B|=a} \sum_{\substack{|C|=a \\ |C \cap B| = a-1}} (n-a-1)!(a-1)! \right) \\ &= \frac{1}{n!} \left(\binom{n}{a} (n-a)!a! + \binom{n}{a} a(n-a) \cdot (n-a-1)!(a-1)! \right) \\ &= 2 \end{aligned}$$

□

Corollary 7.3.5. *The representations $\bigwedge^a \rho^{St,0}$ are irreducible for all $1 \leq a \leq n-1$.*

Proof. We may think of $\bigwedge^a \rho^{St,0}$ as a sub-representation of $\bigwedge^a \rho^{St}$. If

$$\bigwedge^a \rho^{St} = \oplus_i \rho_i^{a_i},$$

is the decomposition into irreducible representations then, by the Lemma,

$$2 = \|\chi\|^2 = \sum_i a_i^2.$$

There is only one possibility, that there are two irreducible representations in $\bigwedge^a \rho^{St}$ and they are non-isomorphic. But then, as $\bigwedge^a \rho^{St,0}$ is a proper sub-representation is must be equal to one of them. □

This is quite useful. For example, for S_5 we get this way 4 irreducible representations of dimensions $4, 6, 4, 1$ (these integers are the values $\dim(\wedge^a \rho^{St,0}) = \binom{4}{a}, a = 1, 2, 3, 4$). They are all distinct, which is clear except for the two 4-dimensional representations where it follows from calculating the characters. The 1-dimensional representation is the sign representation. We also have the trivial representation $\mathbb{1}$. As S_5 has $7 = p(5)$ irreducible representations and their dimensions satisfy $120 = 5! = 1^2 + 1^2 + 4^2 + 6^2 + 4^2 + x^2 + y^2$, we conclude that there are two additional irreducible representations, both of dimension 5. It is not entirely clear how to realize them. See Exercise 24.

7.4. **Tensors, wedges and multi-linear forms.** Let R be a commutative ring. Thus, every R-module is naturally an R-bimodule and so tensor products retain the property of being R-modules. Let V and W be R-modules. An R-d-**multilinear map** of V into W a function

$$f\colon V \times V \times \cdots \times V \to W, \quad (v_1, v_2, \dots, v_d) \to f(v_1, v_2, \dots, v_d),$$

which is R-linear in each variable separately. That is, for any $i = 1, \dots, d$, $v_i, v_i' \in V$, $r, r' \in R$, we have

$$f(v_1, \cdots, rv_i + r'v_i', \dots, v_d) = rf(v_1, \cdots, v_i, \dots, v_d) + r'f(v_1, \cdots, v_i', \dots, v_d).$$

The property

$$f(v_1, \cdots, rv_i, \dots, v_d) = rf(v_1, \cdots, v_i, \dots, v_d)$$

follows from that. A particular case is $d = 2$ giving us the notion of an R-bilinear pairing; note that this a different notion than R-biadditive function, although every R-bilinear pairing is also R-biadditive. Nonetheless, the d-fold tensor product $V^{\otimes d}$ over R serves the same function.

Lemma 7.4.1. *To give an R-d-multilinear map $V^d \to W$ is to give a homomorphism of R-modules*

$$V^{\otimes d} \to W.$$

Proof. Let f be a multilinear map then f is also R-multiadditive and by (a slight extension of) the results we have proven, we get a well-defined homomorphism of abelian groups

$$V^{\otimes d} \to W, \quad v_1 \otimes v_2 \otimes \cdots \otimes v_d \mapsto f(v_1, v_2, \dots, v_d).$$

Now, $r \cdot v_1 \otimes v_2 \otimes \cdots \otimes v_d = (rv_1) \otimes v_2 \otimes \cdots \otimes v_d$ which is mapped to $f(rv_1, v_2, \dots, v_d) = rf(v_1, v_2, \dots, v_d)$. That shows that the map $V^{\otimes d} \to W$ is automatically R-linear. The converse is very similar. □

Let us use the notation

$$V^* := \mathrm{Hom}_R(V, R).$$

Some care is needed because in general $(V^*)^* \neq V$; although there is a natural map $V \to (V^*)^*$ taking $v \in V$ to the function $\varphi \mapsto \varphi(v)$, this map needs not be injective (or surjective). A good case to keep in mind is $R = \mathbb{Z}$, $V = \mathbb{Z}/2\mathbb{Z}$ where $V^* = \{0\}$ and so $V^{**} = \{0\}$ and the map $V \to V^{**}$ is not injective. Nonetheless, in this notation, we find

$$\left\{ \begin{matrix} R\text{-}d\text{-multilinear maps} \\ \text{from } V \text{ to } W \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{homomorphisms of } R\text{-modules} \\ V^{\otimes d} \to W \end{matrix} \right\}$$

We say that an R-d-multilinear map f from V to W is **symmetric** if for any $\sigma \in S_d$ we have

$$f(v_{\sigma(1)}, \dots, v_{\sigma(d)}) = f(v_1, \dots, v_d).$$

Equivalently, if the map $f\colon V^{\otimes d} \to W$ vanishes on the R-submodule spanned by $v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)} - v_1 \otimes \cdots \otimes v_d$.

We say that f is **antisymmetric** if for any $1 \leq i < j \leq d$ we have

$$f(v_1, \dots, v_d) = 0 \text{ if } v_i = v_j.$$

Equivalently, if the map $f\colon V^{\otimes d} \to W$ vanishes on the R-submodule spanned by the tensors $v_1 \otimes \cdots \otimes v_d$ with $v_i = v_j$. This implies that for any $\sigma \in S_d$ we have

$$f(v_{\sigma(1)}, \dots, v_{\sigma(d)}) = \mathrm{sgn}(\sigma) f(v_1, \dots, v_d).$$

Corollary 7.4.2. *There are natural homomorphisms of R-modules*

$$\left\{ \begin{matrix} \textit{R-d-multilinear symmetric maps} \\ \textit{from } V \textit{ to } W \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \textit{homomorphisms of R-modules} \\ \mathrm{Sym}^d V \to W \end{matrix} \right\}$$

and

$$\left\{ \begin{matrix} \textit{R-d-multilinear antisymmetric maps} \\ \textit{from } V \textit{ to } W \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \textit{homomorphisms of R-modules} \\ \bigwedge^d V \to W \end{matrix} \right\}$$

Corollary 7.4.3. *(Uniqueness of determinant) Let V be a free R module of rank d. Up to a scalar, there is a unique d-multilinear anti-symmetric map $V \times \cdots \times V \to R$ (i.e., a determinant map).*

Proof. Such maps correspond to homomorphisms of R modules

$$\bigwedge^d V \to R.$$

But $\bigwedge^d V \cong R$ and $\mathrm{Hom}_R(R, R) = R$. □

Remark 7.4.4. If we choose a basis for V we can represent an element of V by a column vector in R^d and we can represent an element of $V \times \cdots \times V$ (d-times) by a $d \times d$ matrix with entries in R. A d-multilinear antisymmetric map is then a function

$$M_d(R) \to R,$$

that is multilinear in the columns and changes sign when we switch the columns and (even stronger when 2 is not invertible in R) vanishes when two columns are the same. That is, this function has all the properties of the determinant and the Corollary asserts that it must be equal to the determinant up to a sign.

7.4.1. *Existence of invariant forms.* Suppose that G is a finite group acting on a finite dimensional vector space (ρ, V). It is a natural question to ask if there is a non-zero G-invariant bilinear form on V.[6] Using the methods we developed, this is the same as asking if $(\mathrm{Sym}^2(V))^*$ has a G-invariant vector. Now, if χ denotes the character of (ρ, V), the character of $\mathrm{Sym}^2(V)$ is, by Equation (6),

$$\chi_{\mathrm{Sym}^2(V)}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)).$$

Thus, the character ψ of $(\mathrm{Sym}^2(V))^*$ is

$$\psi(g) = \frac{1}{2}(\overline{\chi_V(g)}^2 + \overline{\chi_V(g^2)}).$$

The dimension of the invariant subspace is $\frac{1}{|G|}\sum_{g\in G}\frac{1}{2}(\overline{\chi_V(g)}^2 + \overline{\chi_V(g^2)})$. Since this is an integer, we can take the complex conjugate and conclude:

Proposition 7.4.5. *V has a non-zero G-invariant symmetric bilinear form if and only if*

$$\frac{1}{|G|}\sum_{g\in G}\frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)) \neq 0.$$

More precisely, the dimension of the vector space of invariant symmetric bilinear forms is equal to $\frac{1}{|G|}\sum_{g\in G}\frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2))$.

If V is an irreducible representation of G then using additional considerations – see Exercise 23 – one finds that there is at most one G-invariant bilinear form on V, up to scalar (symmetric or not). Admitting this we conclude:

Corollary 7.4.6. *Let V be an irreducible representation of G. Then there is a symmetric bilinear G-invariant form on V if and only if $\frac{1}{|G|}\sum_{g\in G}\frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)) \neq 0$, in which case this form is unique up-to-scalar.*

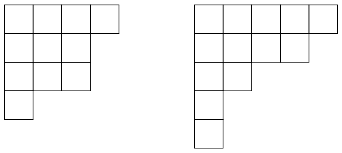
8. Representations of the symmetric group

The representations of the symmetric group are a rich area of research, with a very combinatorial flavour, as to be expected. We will only provide a short introduction, very far from giving a true understanding of this topic.

8.1. **Young tableuax.** Let $n \geq 1$ be an integer and λ be a partition of n that we write as

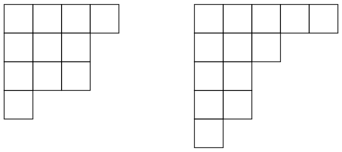
$$\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r),$$

where the λ_i are positive integers whose sum is n. To this partition we associate a **Young diagram** having λ_1 boxes in the first row, λ_2 boxes in the second row and so on. For example, to the partitions $(4,3,3,1)$ and $(5,4,2,1,1)$ we associate the diagrams



[6] We have asked that before for *hermitian* forms, saw that the answer is yes, and put it to good use in proving that every representation decomposes into a direct sum of irreducible representations in Theorem 5.1.2. Although one could address this question using the same methods we are going to use below, it is a bit convoluted and so we will not do it here.

Conversely, a Young diagram defines a partition. If we transpose the Young diagram, making the columns into rows, we get the **conjugate partition** λ'. The conjugate diagrams to those above are, respectively,



corresponding to the conjugate partitions $(4,3,3,1)$ and $(5,3,2,2,1)$, respectively.

A **Young tableau** is obtained by numbering the boxes in the Young diagram using each of the numbers $\{1,2,\dots,n\}$ exactly once. And by doing that we also create a permutation – its cycles are defined by the rows – with associated partition λ.

Here are two Young tableaux associated to the same Young diagram. The first one is called the canonical, or standard, one.

1	2	3
4	5	6
7	8	
9		

2	4	6
3	7	8
9	5	
1		

Given a tableau T there is an associated conjugate tableau T'. Even if T is standard, T' is not standard.

To a Young tableau we associate two subgroups of S_n. They depend on the tableau, not just on the underlying partition λ, but since they depend on the tableau up to conjugation only, we will usually be lax and write these subgroups as P_λ and Q_λ. If you will, they correspond exactly to the standard Young tableau. At any rate:

$$P = P_\lambda = \{\sigma \in S_n : \sigma \text{ preserves every row of the tableau}\}$$

and

$$Q = Q_\lambda = \{\sigma \in S_n : \sigma \text{ preserves every column of the tableau}\}.$$

For example, for the tableau

1	2	3
4	5	6
7	8	
9		

we have

$$P = S_{\{1,2,3\}} \times S_{\{4,5,6\}} \times S_{\{7,8\}}, \quad Q = S_{\{1,4,7,9\}} \times S_{\{2,5,8\}} \times S_{\{3,6\}}.$$

For the tableau

2	4	6
3	7	8
9	5	
1		

we have

$$P = S_{\{2,4,6\}} \times S_{\{3,7,8\}} \times S_{\{5,9\}}, \qquad Q = S_{\{1,2,3,9\}} \times S_{\{4,5,7\}} \times S_{\{6,8\}}.$$

To a partition λ we associate two elements of the group ring of S_n as follows

$$a_\lambda = \sum_{\sigma \in P_\lambda} \sigma, \quad b_\lambda = \sum_{\sigma \in Q_\lambda} \operatorname{sgn} \sigma \cdot \sigma.$$

And we define the **Young symmetrizer** of λ as

$$c_\lambda = a_\lambda b_\lambda \in \mathbb{C}[S_n].$$

If we keep the Young diagram but take another tableau associated to it, the elements $a_\lambda, b_\lambda, c_\lambda$ are instead $\tau a_\lambda \tau^{-1}, \tau b_\lambda \tau^{-1}, \tau c_\lambda \tau^{-1}$ for some $\tau \in S_n$ and any τ will arise this way for some tableau.

Now, the point is that for *every* element y of a group ring $\mathbb{C}[G]$, the right ideal $\mathbb{C}[G]y$ is a left $\mathbb{C}[G]$-module. Thus, it defines a representation of the group G. In fact, the natural map

$$\mathbb{C}[G] \to \mathbb{C}[G]y, \qquad x \mapsto xy,$$

is a homomorphism of representations. Thus, by letting y take different values we get different quotient representations of the regular representation $\mathbb{C}[G]$.

8.2. The irreducible representations V_λ.

Theorem 8.2.1. *Let λ be a partition of n. Then*

$$V_\lambda := \mathbb{C}[S_n] \cdot c_\lambda$$

is an irreducible representation of S_n. Every irreducible representation of S_n is isomorphic to a representation obtained this way, for a unique partition λ.

Proof. We will need a few lemmas. We follow Fulton and Harris.

Lemma 8.2.2. *Let T be a tableau and $P = P_T, Q = Q_T$ be the associated stabilizers, $a = a_T = \sum_{p \in P} p, b = b_T = \sum_{q \in Q} \mathrm{sgn}(q) q, c = c_T = \sum_{(p,q)} \mathrm{sgn}(q) pq$.*

1. *For $p \in P$, $pa = ap = a$ and $pc = c$.*
2. *For $q \in Q$, $qb = bq = \mathrm{sgn}(q)b$ and $cq = \mathrm{sgn}(q)c$.*
3. *For $p \in P, q \in Q$, $pcq = \mathrm{sgn}(q)c$ and, moreover, any element x of $\mathbb{C}[S_n]$ such that $pxq = \mathrm{sgn}(q)x$, for all $p \in P, q \in Q$, is a scalar multiple of c.*

Proof. The first two claims are rather clear given the explicit form of a and b. As $c = ab$ the assertion $pcq = \mathrm{sgn}(q)c$ is clear too. The main issue is to prove that this property characterizes c up to multiplication by a scalar. Let $x \in \mathbb{C}[G]$ be an element such that

$$pxq = \mathrm{sgn}(q)x, \qquad \forall p \in P, q \in Q.$$

Write $x = \sum_g n_g g$. The group G is a disjoint union of double cosets $G = \cup_{g_i} P g_i Q$ and it is clear that the coefficient n_{g_i} determines the coefficient n_g for any $g \in P g_i Q$. For example, if $g = p g_i q$ then, on the one hand, $pxq = \mathrm{sgn}(q)x = \sum_g \mathrm{sgn}(q) n_g g$ and, on the other hand, $pxq = \sum_g n_g pgq$ and we find that

$$n_g = \mathrm{sgn}(q) n_{g_i}, \ \text{ if } g = p g_i q. \tag{7}$$

For example, for $g = pq \in PQ$ we have

$$n_g = n_1 \cdot \mathrm{sgn}(q).$$

Note that $P \cap Q = \{1\}$ as any permutation fixing every row and every column of a Young tableau fixes all its entries. And so, *defining*, $n_g = n_1 \cdot \mathrm{sgn}(q)$, and $n_g = 0$ for all $g \notin PQ$, is well-defined and gives us, in fact, $n_1 \cdot c$.

What remains to prove is that if $g \notin PQ$ then $n_g = 0$. If $g \notin PQ$ we will prove that $n_g = 0$ by finding a transposition τ such that $\tau \in P, g^{-1}\tau g \in Q$. Then, using Equation (7),

$$n_g = n_{\tau \cdot g \cdot g^{-1}\tau g} = \mathrm{sgn}(g^{-1}\tau g) n_g = -n_g,$$

and so

$$n_g = 0.$$

How can we find such a transposition? Let us be more precise and let T be the standard Young tableau associated to λ. The subgroups P, Q and the elements a, b, c are really P_T, Q_T, a_T, b_T, c_T. Let us consider the tableau gT obtained by applying g to every entry of T. We have

$$P_{gT} = g P_T g^{-1}, \quad Q_{gT} = g Q_T g^{-1}.$$

We claim that if $g \notin PQ$ then there is a pair of integers $i \neq j$ such that i, j appear in the same row of T and in the same column of gT. Given that, choose $\tau = (ij)$. Then, as i, j, are in the same row of T, definitely $\tau \in P_T$. As i, j, are in the same column of gT, definitely $\tau \in Q_{gT}$ and so $g^{-1}\tau g \in Q_T$. Thus, we are done once we prove the following lemma:

Lemma 8.2.3. *Suppose that there is no pair of distinct integers that appear in the same row of T and the same column of gT then $g \in PQ$.*

Before proving the lemma, it may be a good illustration to look at a particular example. Consider the following Young tableau

$$T = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & 6 \\ \hline 7 & 8 & \\ \cline{1-2} 9 & & \\ \cline{1-1} \end{array}$$

We $P_T = S_{\{1,2,3\}} \times S_{\{4,5,6\}} \times S_{\{7,8\}}, Q_T = S_{\{1,4,7,9\}} \times S_{\{2,5,8\}} \times S_{\{3,6\}}$. Let us take $g = (15)(37)$. Then

$$gT = \begin{array}{|c|c|c|} \hline 5 & 2 & 7 \\ \hline 4 & 1 & 6 \\ \hline 3 & 8 & \\ \cline{1-2} 9 & & \\ \cline{1-1} \end{array}$$

Then $1, 2$ appear in the same row of T and same column of gT ($4, 5$ are another example). On the other hand, let us take an element g that is clearly in $P_T Q_T$, say $g = (123)(78)(1479) = (14879231)$. Then,

$$gT = \begin{array}{|c|c|c|} \hline 4 & 3 & 1 \\ \hline 8 & 5 & 6 \\ \hline 9 & 7 & \\ \cline{1-2} 2 & & \\ \cline{1-1} \end{array}$$

We can verify that there is no pair of integers that appears in the same row of T and the same column of gT. The lemma states that this, in turn, implies that $g \in PQ$.

Proof. (Lemma 8.2.3) We can find $p \in P$ and $q \in Q_{gT}$ such that gT and $q(gT)$ have the same first row. Indeed, find q by "raising to the top" in each column of gT the elements appearing in the first row of T and use p to rearrange the first row of T so that pT and $q(gT)$ have the same first row. This is possible to do because of the assumption that no two integers appear in the same row of T and the same column of gT – in particular, the integers in the first row of T are in different columns of gT and so in each column of gT there is precisely one integer from the first row of T.

In the example above, we can take $q = (9842)$ and $p = (123)$. Then

$$pT = \begin{array}{|c|c|c|} \hline 2 & 3 & 1 \\ \hline 4 & 5 & 6 \\ \hline 7 & 8 & \\ \cline{1-2} 9 & & \\ \cline{1-1} \end{array} \qquad q(gT) = \begin{array}{|c|c|c|} \hline 2 & 3 & 1 \\ \hline 4 & 5 & 6 \\ \hline 8 & 7 & \\ \cline{1-2} 9 & & \\ \cline{1-1} \end{array}$$

Now consider the tableaux $pT, q(gT)$, where we erase the first row. Their, P and Q, so to say, satisfy $P \subset P_T, Q \subset Q_T$. And we can repeat the process getting a p', q' (in our example, $p' = Id, q' = Id$) and pass to third row to find p'', q'', and so on. In our example, we will then use $p'' = (78), q'' = Id$.

Thus, we can find $p \in P, q \in Q_{gT}$ such that $pT = q(gT)$. This implies that $p = qg$, or $pg^{-1}q^{-1} = 1$ and

$$g = p \cdot g^{-1}q^{-1}g \in P_T \cdot g^{-1}Q_{gT}g = P_T Q_T.$$

$\square$

$\square$

Corollary 8.2.4. *For any $z \in \mathbb{C}[S_n]$ we have $c_\lambda z c_\lambda \in \mathbb{C}c_\lambda$. In particular, $c_\lambda^2 = n_\lambda c_\lambda$ for some $n_\lambda \in \mathbb{C}$.*

Proof. (Corollary) Let $x = c_\lambda z c_\lambda$. For $p \in P, q \in Q$, we have $pxq = (pc_\lambda)z(c_\lambda q) = \mathrm{sgn}(q)c_\lambda z c_\lambda = \mathrm{sgn}(q)x$. Thus, x is a scalar multiple of c_λ. $\square$

We can now prove that $V_\lambda = \mathbb{C}[S_n]c_\lambda$ is an irreducible representation:

It follows from the Corollary that $c_\lambda V_\lambda \subseteq \mathbb{C}c_\lambda$. Let W be a subrepresentation of V_λ and consider $c_\lambda W$. There are two possibilities.

- $c_\lambda W = \mathbb{C}c_\lambda$. This means that $c_\lambda = c_\lambda w$ for some $w \in W$. Then $V_\lambda = \mathbb{C}[S_n]c_\lambda = \mathbb{C}[S_n]c_\lambda w \subseteq \mathbb{C}[S_n]w \subseteq \mathbb{C}[S_n]W \subseteq W$ and so $W = V_\lambda$.
- $c_\lambda W = \{0\}$. In this case we want to show that $W = \{0\}$. We need a lemma.

Lemma 8.2.5. *Let G be a finite group and let W be isomorphic to a subrepresentation of $\mathbb{C}[G]$. For example, any irreducible representation of G has this property. There exists an element $\varphi \in \mathbb{C}[G]$ such that $W \cong \mathbb{C}[G]\varphi$ as a $\mathbb{C}[G]$-module. Moreover, $\varphi^2 = \varphi$.*

Proof. We know that W is isomorphic to a subrepresentation of $\mathbb{C}[G]$, and so we may assume that W is already a subrepresentation of $\mathbb{C}[G]$. We can therefore decompose $\mathbb{C}[G]$, *as a* $\mathbb{C}[G]$*-module*, as

$$\mathbb{C}[G] = W \oplus W^\perp,$$

and let φ_W be the projection map $\mathbb{C}[G] \rightarrow W$, which is a map of $\mathbb{C}[G]$-modules. Now, consider the element $1 \in \mathbb{C}[G]$ and its decomposition

$$1 = \varphi + \sigma.$$

Obviously, $\varphi_W(1) = \varphi_W(\varphi) + \varphi_W(\sigma) = \varphi$. Therefore, $\varphi_W(\tau) = \tau\varphi_W(1) = \tau\varphi$. That is, the projection map φ_W is multiplication from the right by φ. Since φ_W is a projection, $\varphi_W^2 = \varphi_W$ and so $\varphi_W^2(1) = \varphi_W(1)$; equivalently, $\varphi^2 = \varphi$. □

We return now to the case of the symmetric group and $W \subseteq V_\lambda$ such that $c_\lambda W = 0$. Then $W \cdot W \subseteq (\mathbb{C}[G]c_\lambda) \cdot W = \mathbb{C}[G] \cdot (c_\lambda W) = 0$. On the other hand, for φ as in Lemma 8.2.5, $\varphi = \varphi^2 \in W \cdot W$ and we get a contradiction, unless $\varphi = 0$. Namely, unless $W = \{0\}$.

That concludes the proof that V_λ is irreducible.

We note several consequences of the considerations above:

- Taking the case $W = V_\lambda$, we get that $c_\lambda V_\lambda \neq \{0\}$ and so $c_\lambda V_\lambda = \mathbb{C}c_\lambda$.
- $c_\lambda^2 = n_\lambda c_\lambda$ for some $n_\lambda \in \mathbb{C}$ (already from Corollary 8.2.4).
- Consider the linear operator T, which is the multiplication from the right by c_λ:

$$\mathbb{C}[S_n] \rightarrow \mathbb{C}[S_n], \qquad x \mapsto xc_\lambda.$$

As

$$c_\lambda = \sum_{(p,q)\in P\times Q} \mathrm{sgn}(q) \cdot pq,$$

for every $\sigma \in S_n$ we have

$$T(\sigma) = \sigma c_\lambda = \sum_{(p,q)\in P\times Q} \mathrm{sgn}(q) \cdot \sigma pq.$$

From this we find that if we calculate the trace of T using the standard basis for $\mathbb{C}[S_n]$ then

$$\mathrm{Tr}(T) = n!$$

Now, the kernel of T, $\mathrm{Ker}(T)$, is a $\mathbb{C}[S_n]$-submodule of $\mathbb{C}[S_n]$ and the image of T, V_λ, is irreducible. If $V_\lambda \cap \mathrm{Ker}(T) \neq 0$ then in fact $V_\lambda \subseteq \mathrm{Ker}(T)$ and that implies $T^2 = 0$. But then the characteristic polynomial of T is $x^{n!}$ and in particular $\mathrm{Tr}(T) = 0$. Contradiction. Thus, $\mathrm{Ker}(T)$ doesn't intersect V_λ. On the other hand, the dimension of $V_\lambda = n! - \dim(\mathrm{Ker}(T))$. Therefore, there is a direct sum decomposition as $\mathbb{C}[S_n]$ modules:

$$\mathbb{C}[S_n] = \mathrm{Ker}(T) \oplus V_\lambda.$$

It follows that $\mathrm{Tr}(T) = \dim(V_\lambda) \cdot n_\lambda$ because T acts on V_λ by multiplication by n_λ. We conclude that $n_\lambda = n!/\dim(V_\lambda)$, a rational number.[7]

- Consequently, we find that
$$(\frac{1}{n_\lambda}c_\lambda)^2 = \frac{1}{n_\lambda}c_\lambda.$$
We conclude that in fact $\frac{1}{n_\lambda}c_\lambda$ is the idempotent defining V_λ, whose existence is guaranteed by Lemma 8.2.5.

To complete the proof of Theorem 8.2.1 we need to also prove that if $\lambda \neq \mu$ then $V_\lambda \ncong V_\mu$.

Write $\lambda = (\lambda_1 \geq \lambda_2 \geq \dots), \mu = (\mu_1 \geq \mu_2 \geq \dots)$. We say that $\lambda > \mu$ is the first non-vanishing difference $\lambda_i - \mu_i > 0$. This provides a linear (lexicographic) order on S_n; for every $\lambda \neq \mu$ either $\lambda > \mu$ or $\mu > \lambda$.

Lemma 8.2.6. *If $\lambda < \mu$ then $c_\lambda \mathbb{C}[G]c_\mu = 0$ and in particular $c_\lambda c_\mu = 0$.*

Note that the lemma implies that $V_\lambda \ncong V_\mu$ for $\lambda \neq \mu$. Indeed, if they are isomorphic, we may assume $\lambda < \mu$ and then, on the one hand $c_\lambda V_\lambda \neq 0$, and on the other hand, $c_\lambda V_\lambda \cong c_\lambda \mathbb{C}[G]c_\mu = 0$. So it's enough to prove the lemma.

To prove the lemma, it suffices to prove that for all $g \in \mathbb{C}[S_n]$ we have $b_\lambda g a_\mu = 0$ and, in fact, it suffices to prove that for $g \in S_n$. It is thus enough to prove $b_\lambda \cdot g a_\mu g^{-1} = 0$. One way to think about it is that we can change the tableau T' used to construct a_μ from T' to gT'. So, it is enough to prove that
$$b_T a_{T'} = 0,$$
where T is the tableau used to define b_λ (that we can assume to be a standard tableau) and T' the tableau used to define a_μ, without assuming it to be standard.

The assumption that $\lambda < \mu$ implies that there are two integers $i \neq j$ that are in the same column of λ and the same row of T'. To prove that we introduce some (non-standard) terminology. We will denote by $T[i]$ the i-th row of a tableau T and by ctnt($T[i]$) the numbers appearing in it.

The proof is by induction on n, where the case $n = 2$ is clear as there is only one possibility for $\lambda < \mu$ then, corresponding to the tableaux
$$T = \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline \end{array} \qquad T' = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline \end{array}$$
Consider the case $n > 2$, and denote $\lambda = (\lambda_1 \geq \dots \geq \lambda_r), \mu = (\mu_1 \geq \dots \geq \mu_s)$. If $\lambda_1 < \mu_1$ then ctnt($T'[1]$), that consists of μ_1 numbers, is distributed over the λ_1 columns of T and so there are $i \neq j$ in the first row of T' that are in the same column of T.

Suppose that $\lambda_1 = \mu_1$, and suppose that ctnt($T'[1]$) is distributed over all λ_1 columns of T (if this is not the case, then there are $i \neq j$ in the first row of T' that are in the same column of T and we are done). There exist then $q \in Q_T$ such that ctnt($T'[1]$) = ctnt($qT[1]$). Consider then the tableaux
$$qT^* = (qT[2], \dots, qT[r]), \qquad T'^* = (T'[2], \dots, T'[s]),$$
that are associated with the set $S^* = \{1, \dots, n\} \setminus$ ctnt($T'[1]$), whose size n^* is smaller that n, and the partitions $\lambda^* = (\lambda_2 \geq \dots \geq \lambda_r), \mu^* = (\mu_2 \geq \dots \geq \mu_s)$. Note that $\lambda^* < \mu^*$, which implies $n^* \geq 2$. Applying the induction hypothesis, there are $i \neq j$ appearing in the same row of T'^* and the same column of qT^*. But that also means that i, j appear in the same column of T.

[7] In fact, an integer as the dimension of an irreducible representation divides the order of the group. We will not need this.

Thus, if these integers are i, j then $\tau = (ij) \in Q_T \cap P_{T'}$ and
$$b_T a_{T'} = (b_T \tau)(\tau a_{T'}) = -b_T a_{T'},$$
and we conclude $a_T b_{T'} = 0$. □

Example 8.2.7. Consider the trivial Young tableau

$$\begin{array}{|c|c|c|c|c|}\hline 1&2&3&\dots&n\\\hline\end{array}$$

In this case $P = S_n, Q = \{1\}$ and so $a = \sum_{\sigma\in S_n} \sigma, b = 1$ and $c = \sum_{\sigma\in S_n} \sigma$. Note that for every σ we have $\sigma c = c$. Namely, $\mathbb{C}[S_n] \cdot c = \sum_\sigma \mathbb{C}\sigma c = \mathbb{C}c$, with every σ active trivially. That is, the associated representation is the trivial representation.

Example 8.2.8. Consider the Young tableau

$$\begin{array}{|c|}\hline 1\\\hline 2\\\hline 3\\\hline \vdots\\\hline n\\\hline\end{array}$$

In this case $P = \{1\}, Q = S_n$ and so $a = 1, b = c = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\cdot\sigma$. Note that for every σ we have $\sigma c = \operatorname{sgn}(\sigma)c$. Therefore, $\mathbb{C}[S_n] \cdot c = \sum_\sigma \mathbb{C}\sigma c = \mathbb{C}\operatorname{sgn}(\sigma)c = \mathbb{C}c$. Thus, the associated representation is just the 1-dimensional sign representation.

Example 8.2.9. A somewhat more complicated example is coming from the Young tableau

$$\begin{array}{|c|c|c|c|c|}\hline 1&2&3&\dots&n-1\\\hline n\\\cline{1-1}\end{array}$$

We claim that the associated representation is $\rho^{St,0}$. More generally, the representation associated to the tableau

$$\begin{array}{|c|c|c|c|c|}\hline 1&2&3&\dots&n-s\\\hline n-s+1\\\cline{1-1} \vdots\\\cline{1-1} n-1\\\cline{1-1} n\\\cline{1-1}\end{array}$$

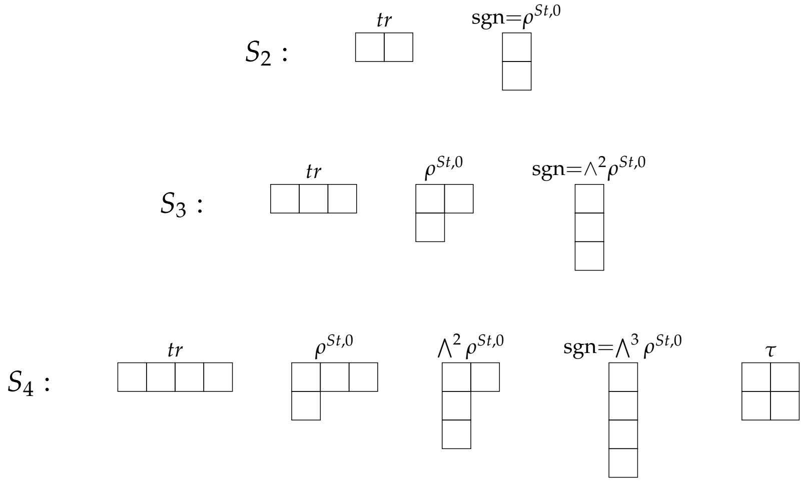
is $\bigwedge^s \rho^{St,0}$. Let us sketch the argument for the case $s = 1$. In this case
$$P = S_{n-1}, \quad Q = \langle (1n) \rangle,$$
and
$$a = \sum_{\sigma\in S_{n-1}} \sigma, \qquad b = 1 - (1n), \qquad c = \sum_{\sigma\in S_{n-1}} \sigma - \sum_{\sigma\in S_{n-1}} \sigma\cdot(1n).$$
Now, quite generally, given a representation V of a group G, choose a vector $v \in V$, $v \neq 0$, and define
$$\mathbb{C}[G] \to V, \quad x \mapsto xv.$$
This is a morphism of $\mathbb{C}[G]$ modules. Given a left ideal I of $\mathbb{C}[G]$, I is a $\mathbb{C}[G]$ module and the map $\mathbb{C}[G] \to V$ induces a map of $\mathbb{C}[G]$-modules
$$I \to V, \quad x \mapsto xv.$$
If V is irreducible, the morphism $I \to V$ is either surjective, or zero. If I is irreducible, the map is either injective or zero.

Let us take the ideal $I = \mathbb{C}[S_n]c$ and the vector $v = (1, 1, \dots, -n-1) \in \rho^{St,0}$. Apply b to it: $bv = (n, 0, \dots, -n)$. Apply a to get $abv = (t, t, \dots, t, -n\cdot(n-1)!)$, where $t = n\cdot(n-2)!$. In particular abv is not zero. Thus, we have a surjection
$$\mathbb{C}[G]c \twoheadrightarrow \rho^{St,0}.$$

Since we know V_λ is irreducible, the map is an isomorphism.

To show this is an isomorphism without using that V_λ is irreducible, it is enough to show that $\dim(\mathbb{C}[G]c) \leq n-1$. Using that for every $\sigma \in S_{n-1}$ we have $\sigma a = a$ and so $\sigma c = c$, we find that $\mathbb{C}[G]c = \sum_{i=1}^n \mathbb{C} \cdot (in)c$, and then using that $(\sum_{i=1}^n (in))a = \sum_{\sigma \in S_n} \sigma$ we also find that $(\sum_{i=1}^n (in))c = 0$. It follows that $\dim(\mathbb{C}[G]c) \leq n-1$, as desired.

Assuming the result for $\bigwedge^s \rho^{st,0}$ we can match the Young diagrams with representations, at least for $n \leq 4$.

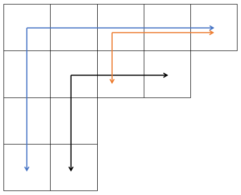


τ is the representation $\rho^{St,0}$ of S_3, pulled-back to S_4 through the homomorphism $S_4 \to S_3$.

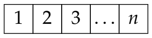
8.3. **Further results.** As one suspects, there is a lot of combinatorics involved in understanding what are the properties of the representations arising as $\mathbb{C}[G]c_\lambda$ (and some key words to google are "tabloid" and "Specht module"). For example, the dimension of the representation $V_\lambda = \mathbb{C}[G]c_\lambda$ is given by the **hook length formula**

$$\dim(V_\lambda) = \frac{n!}{\prod_{\text{all hooks}} (\text{hook length})}.$$

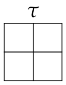
Every box in a Young diagram has a **hook** associated to it that consists off all boxes to the right of the box (and in the same row) and all boxes below the box (in the same column), including the initial box itself.



A diagram thus has n hooks. The **hook length** is just the number of the boxes in the hook. In the diagram above, 3 hooks are indicated and their lengths are 8, 5 and 4. The diagram



has n hooks, of lengths $n, n-1, \ldots, 1$. The dimension of the associated representation should therefore be 1 and we know that is correct. The diagram



has hooks of length $3, 2, 2, 1$, giving a representation of dimension $4!/(3 \times 2 \times 2) = 2$.

A more general, and very natural, question is what is the character χ_λ of the representation V_λ? A formula for χ_λ will provide a formula for the dimension as $\dim(V_\lambda) = \chi_\lambda(1)$.

Let $g \in S_n$ be a permutation of cycle type $(i_1, \dots, i_n)$ – meaning it has i_1 cycles of length 1, i_2 cycles of length 2, ..., i_n cycles of length n (and so $\sum_{j=1}^n j \cdot i_j = n$). Don't confuse that with the partition associated to g. Also use the notation $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k)$ for the partition λ. Define then

$$\ell_1 = \lambda_1 + k - 1, \ell_2 = \lambda_2 + k - 2, \dots, \ell_k = \lambda_k.$$

And define polynomials $P_1, \dots, P_n$ in the variables $x_1, \dots, x_k$, by

$$P_j(x) = x_1^j + x_2^j + \cdots + x_k^j.$$

Let also,

$$\Delta(x) = \prod_{1 \leq i < j \leq k} (x_i - x_j).$$

Frobenius' formula. *The character χ_λ is given by*

$$\chi_\lambda(g) = \textit{coefficient of } \; x_1^{\ell_1} \cdots x_k^{\ell_k} \; \textit{ in the polynomial } \; \Delta(x) \cdot \prod_{j=1}^n P_j(x)^{i_j}.$$

We will not prove this formula in this course. The proof can be found in Fulton & Harris.

9. Representations of $\mathrm{GL}_2(\mathbb{F})$, $\mathbb{F}$ a finite field.

✠ This particular section was not proof-read ✠

To find all the complex representations of $\mathrm{GL}_2(\mathbb{F})$, where $\mathbb{F}$ is a finite field of $q = p^r$ elements, we begin by first determining the conjugacy classes. We will assume that $char(\mathbb{F}) \neq 2$.

9.1. **Conjugacy classes in** $\mathrm{GL}_2(\mathbb{F})$.

Recall a consequence the structure theorem for modules over PID. Matrices in $\mathrm{GL}_n(\mathbb{F})$ are classified up to conjugacy by their rational canonical form. For $\mathrm{GL}_2(\mathbb{F})$ the rational canonical forms corresponds to pairs of polynomials of the form $\{(x-a, x-a), a \in \mathbb{F}^\times\}$ of which there are $q-1$, to pairs of polynomials of the form $(x-a, x-b), a \neq b \in \mathbb{F}^\times$ of which there are $(q-1)(q-2)/2$, to polynomials of the form $(x-a)^2, a \in \mathbb{F}^\times$ of which there are $q-1$, and to quadratic irreducible polynomials $x^2 + ax + b, a \in \mathbb{F}, b \neq 0 \in \mathbb{F}$ of which there are $q(q-1) - (q-1) - (q-1)(q-2)/2 = q(q-1)/2$. These correspond to $\mathbb{F}[x]$-modules of the form

$$\mathbb{F}[x]/(x-a) \oplus \mathbb{F}[x]/(x-a), \quad \mathbb{F}[x]/(x-a) \oplus \mathbb{F}[x]/(x-b), \quad \mathbb{F}[x]/((x-a)^2), \quad \mathbb{F}[x]/(x^2+ax+b).$$

Examples of such matrices are provided by

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \quad \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}.$$

The centralizer of a matrix corresponds to the automorphism group of the module. Thus, in the first case the centralizer is $\mathrm{GL}_2(\mathbb{F})$, in the second case it is $\{\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right) : x, y \in \mathbb{F}^\times\}$, in the third case it is $\{\left(\begin{smallmatrix} x & y \\ & x \end{smallmatrix}\right) : x \in \mathbb{F}^\times, y \in \mathbb{F}\}$ and in the fourth case it is the units of $\mathbb{F}[x]/(x^2+ax+b)$ which is a group of order $q^2 - 1$. This allows us, by the orbit-stabilizer formula, to determine how many elements are in each conjugacy class and we find the following:

rational form type	representative	no. of classes	size of conj. class
$(x-a, x-a)$	$\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$	$q-1$	1
$(x-a, x-b)$	$\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$	$(q-1)(q-2)/2$	$q(q+1)$
$(x-a)^2$	$\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$	$q-1$	q^2-1
x^2+ax+b	$\left(\begin{smallmatrix} 0 & -b \\ 1 & -a \end{smallmatrix}\right)$	$q(q-1)/2$	q^2-q
		$= q^2-1$	

Thus, we must find q^2-1 distinct irreducible representations of $\mathrm{GL}_2(\mathbb{F})$. The simplest are the one dimensional characters. There are $q-1$ distinct homomorphisms $\alpha\colon \mathbb{F}^\times \to \mathbb{C}^\times$. Composing them with the determinant we find $q-1$ distinct one dimensional characters

$$\alpha(\det)\colon \mathrm{GL}_2(\mathbb{F}) \to \mathbb{C}^\times.$$

(In fact these are all the 1-dimensional characters. Equivalently, the commutator of $\mathrm{GL}_2(\mathbb{F})$ is $\mathrm{SL}_2(\mathbb{F})$, in fact for any field $\mathbb{F}$ and also for $\mathrm{GL}_n(\mathbb{F})$. But we will not need this fact.) We call the corresponding one dimensional representations U_α.

9.2. **Representations induced from a Borel.**

Let B be the Borel subgroup of $\mathrm{GL}_2(\mathbb{F})$ that consists of the upper triangular matrices:

$$B = \left\{ \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} : a, b \in \mathbb{F}^\times, x \in \mathbb{F} \right\}.$$

It is a subgroup of $\mathrm{GL}_2(\mathbb{F})$ of index $q+1$. The 1-dimensional characters of B are all of the form

$$\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \mapsto \alpha(a)\beta(b),$$

where α, β are characters of $\mathbb{F}^\times$. We denote these characters

$$\chi_{\alpha,\beta}\colon B \to \mathbb{F}^\times.$$

Define

$$W_{\alpha,\beta} = \mathrm{Ind}_B^{\mathrm{GL}_2(\mathbb{F})} \chi_{\alpha,\beta}.$$

It is a representation of $\mathrm{GL}_2(\mathbb{F})$ of dimension $q+1$.

Lemma 9.2.1. *If $\alpha \neq \beta$, $W_{\alpha,\beta}$ is irreducible. If $\alpha = \beta$ then $W_{\alpha,\alpha}$ is reducible and $W_{\alpha,\beta} = U_\alpha \oplus V_\alpha$, where V_α is an irreducible q dimensional representation. The representation $W_{\alpha,\beta}$ determines the unordered pair of characters $\{\alpha, \beta\}$ and the representation V_α determines the character α.*

Proof. We use Theorem 4.2.1 to calculate the induced character. For example, for an element of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, there is a unique conjugate of it in B (i.e, itself) if $a = b$. And for $a \neq b$ it has $2q$ conjugates in B (the matrices $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix}$, for any x, and the matrices $\begin{pmatrix} b & x \\ 0 & a \end{pmatrix}$, for any x). In the first case the size of the centralizer is $(q^2-1)(q^2-q)$ (the size of $\mathrm{GL}_2(\mathbb{F})$) and in the second case the size of the centralizer is $(q-1)^2$ for each of the cases. Thus, the value of the induced character is $(q+1)(\alpha(a)\beta(a))$ in the first case, and $\alpha(a)\beta(b) + \alpha(b)\beta(a)$ in the second case. We leave the calculation of the remaining cases as an exercise.

The character of $W_{\alpha,\beta}$ is given according to conjugacy classes as follows

$(x-a,x-a)$	$(x-a,x-b)$	$(x-a)^2$	x^2+ax+b
$(q+1)\alpha(a)\beta(a)$	$\alpha(a)\beta(b)+\beta(a)\alpha(b)$	$\alpha(a)\beta(a)$	0

Not that the character determines the pair $\{\alpha,\beta\}$. Now, as α,β take their values in roots unity, we have

$$\begin{aligned}\|\mathrm{Ind}\chi_{\alpha,\beta}\|^2 &= \frac{1}{(q^2-1)(q^2-q)}\Big(\sum_{a\in\mathbb{F}^\times}(q+1)^2+q(q+1)\sum_{\{a\neq b\}\subset\mathbb{F}^\times}(2+\alpha(a/b)\beta(b/a)+\alpha(b/a)\beta(a/b))+(q^2-1)\sum_{a\in\mathbb{F}^\times}1\Big)\\ &= \frac{1}{(q^2-1)(q^2-q)}[(q-1)(q+1)^2+q(q+1)(q-1)(q-2)+\\ &\qquad \frac{q(q+1)}{2}\sum_{\{(a,b):a\neq b,ab\neq 0\}}(\alpha(a/b)\beta(b/a)+\alpha(b/a)\beta(a/b))+(q^2-1)(q-1)].\end{aligned}$$

Now, use that for any group G and a non-trivial one dimensional character χ of G, $\sum_{g\in G}\chi(g)=0$, to deduce that if $\alpha\neq\beta$, then $\sum_{(a,b)}\alpha(a/b)\beta(b/a)=0$. We then get

$$\begin{aligned}\|\mathrm{Ind}\chi_{\alpha,\beta}\|^2 &= \frac{1}{(q^2-1)(q^2-q)}[(q-1)(q+1)^2+q(q+1)(q-1)(q-2)-\frac{q(q+1)}{2}\sum_{a\in\mathbb{F}^\times}2+(q^2-1)(q-1)]\\ &= \frac{1}{(q^2-1)(q^2-q)}[(q-1)(q+1)^2+q(q+1)(q-1)(q-2)-q(q+1)(q-1)+(q^2-1)(q-1)]\\ &= 1.\end{aligned}$$

Now, if $\alpha=\beta$ then

$$\begin{aligned}\|\mathrm{Ind}\chi_{\alpha,\beta}\|^2 &= \frac{1}{(q^2-1)(q^2-q)}[(q-1)(q+1)^2+q(q+1)(q-1)(q-2)+2q(q+1)(q-1)(q-2)+(q^2-1)(q-1)]\\ &= 2.\end{aligned}$$

It follows that $W_{\alpha,\alpha}$ is a sum of two irreducible representations. We claim that the representation $\alpha\circ\det$ appears in $W_{\alpha,\alpha}$. To show that we can use Frobenius reciprocity

$$\mathrm{Hom}_G(W_{\alpha,\alpha},\alpha\circ\det)\cong\mathrm{Hom}_H(\chi_{\alpha,\alpha},\alpha\circ\det|_H).$$

But $\chi_{\alpha,\alpha}=\alpha\circ\det|_H$, so the r.h.s. is non-zero. We conclude that

$$W_{\alpha,\alpha}=\alpha(\det)\oplus V_\alpha,$$

where V_α is irreducible of dimension q with character Note that the character determines α. □

$(x-a,x-a)$	$(x-a,x-b)$	$(x-a)^2$	x^2+ax+b
$q\alpha(a^2)$	$\alpha(ab)$	0	$-\alpha(b)$

So far, we found the following distinct irreducible representations:

(1) $q-1$ 1-dimensional representations $\alpha(\det)$.
(2) $(q-1)(q-2)/2$ $q+1$-dimensional representations.
(3) $q-1$ q-dimensional representations.

We are therefore missing $q^2-1-(q-1+(q-1)(q-2)/2+q-1)=q(q-1)/2$ irreducible representations. If they all the same dimension that dimension should be $q-1$.

Let $\epsilon\in F^\times$ be a non-square. Then $F[x]/(x^2-\epsilon)$ is a field with q^2 elements that we denote L. Writing

$$L=F\oplus F\sqrt{\epsilon},$$

multiplication becomes an F-linear transformation. $a \in F$ acts by the diagonal matrix $\mathrm{diag}(a, a)$ and $b\sqrt{\epsilon}$ for $b \in F$ acts by the matrix $\left(\begin{smallmatrix} 0 & b\epsilon \\ b & 0 \end{smallmatrix}\right)$. We get a homomorphism

$$L^\times \to \mathrm{GL}_2(F), \qquad \zeta := a + b\sqrt{\epsilon} \mapsto \left(\begin{smallmatrix} a & b\epsilon \\ b & a \end{smallmatrix}\right).$$

Following Fulton and Harris we will call the image K, but think of ζ also as an element of K. The elements in K such that $b \neq 0$ are elements of L that are not in F. The characteristic polynomial of such elements and its discriminant Δ are the following

$$t^2 - 2at + (a^2 - b^2\epsilon), \qquad \Delta = 4b^2\epsilon.$$

As ϵ is not a square, this is an irreducible polynomial. We observe that we get all the irreducible quadratic monic polynomials in $F[x]$ this way. Therefore, the $(q^2 - q)/2$ pairs of elements of K, $\zeta = a \pm b\sqrt{\epsilon}$ for which $b \neq 0$ are representatives to the conjugacy classes of matrices with irreducible characteristic polynomial.

The group K is a cyclic group and we can take any of its $q^2 - 1$ characters $\varphi \colon K \to \mathbb{C}^\times$. When we look at $\mathrm{Ind}_K^G \varphi$ we get a $q^2 - q$-dimensional representation whose character is given as follows.

$(x-a, x-a)$	$(x-a, x-b)$	$(x-a)^2$	$\zeta = a \pm b\sqrt{\epsilon}$
$q(q-1)\varphi(x)$	0	0	$\varphi(\zeta) + \varphi(\zeta^q)$

The argument is easy: the only elements of K with reducible characteristic polynomial are the diagonal matrices $\mathrm{diag}(a, a), a \in F^\times$. The only conjugates of $\zeta = a + b\sqrt{\epsilon}$ that lie in K are $a \pm b\sqrt{\epsilon}$.

At this point, we are going to pull a rabbit out of a hat. Suppose that $\varphi \neq \varphi^q$ and consider the class function χ^φ (a notation we choose so as to show the dependence on φ, yet to distinguish it from the character of φ, which is φ, and from the character of $\mathrm{Ind}_K^G \varphi$.

$$\chi_{V_1 \otimes W_{\alpha,1}} - \chi_{W_{\alpha,1}} - \chi_{\mathrm{Ind}_K^G \varphi}.$$

It has the following values on conjugacy classes

$(x-a, x-a)$	$(x-a, x-b)$	$(x-a)^2$	$\zeta = a \pm b\sqrt{\epsilon}$
$(q-1)\varphi(a)$	0	$-\varphi(a)$	$-\varphi(\zeta) - \varphi(\zeta^q)$

Also $\|\chi^\varphi\|^2 = 1$ and $\chi^\varphi(1) = q - 1 > 0$. If we write φ as an $\mathbb{Z}$-linear combination of the irreducible characters, possibly with negative coefficients, we can deduce that in fact φ is an irreducible character, corresponding to an irreducible representation X_φ. Note that φ and φ^q give the same character, but that is the extent of the identifications. There are $q - 1$ characters φ such that $\varphi = \varphi^q$ and $(q^2 - 1) - (q - 1)$ such that $\varphi \neq \varphi^q$. Thus, we get $(q^2 - q)/2$ irreducible representations of dimension $q - 1$. By looking at the character tables we can recognize that all the irreducible representations we have constructed are non-isomorphic. Therefore, we found all the complex irreducible representations for $\mathrm{GL}_2(F)$, where F is a finite field.

Part 4. Categories and functors II

Category theory is not for everyone. However, some of its concepts are absolutely fundamental to a growing list of areas in mathematics, among which algebraic, complex and differential geometry, topology, algebra with all its branches are among the main customers. In this section we will touch on several such concepts. The first is Yoneda's lemma that says that an object in a category is determined by its "points". This concept is critical in the theory of moduli spaces, classifying spaces and so on. We will then revisit the notion of equivalence of categories and prove two results: the first is a criterion for a functor to be an equivalence of categories (and most of the time, this is how one proves in "real life" that two categories are equivalent), the other is an example called Morita equivalence that states that for a ring R the category of modules over R and $M_n(R)$ are equivalent. And so, if R is a division ring we conclude that this is a unique irreducible module over $M_n(R)$ and it is simply R^n. After that, we are going to provide a precise explanation of the meaning of the statement that certain objects have a universal property. We will apply that for example to tensor products, but also on the basis of this we will discuss limits in a category. Limits are very interesting processes: they will provide us with a good definition of infinite Galois groups, of p-adic numbers, of fibre products and so on.

10. Yoneda's lemma

Let $\mathbf{C}$ be a category. Given an object A in $\mathbf{C}$ we can define two functors associated with it. A covariant functor

$$h_A\colon \mathbf{C} \to \mathbf{Sets}, \quad h_A(B) = \mathrm{Mor}_{\mathbf{C}}(A,B);$$

a contraviant functor

$$h^A\colon \mathbf{C} \to \mathbf{Sets}, \quad h^A(B) = \mathrm{Mor}_{\mathbf{C}}(B,A).$$

We will prove that the isomorphism class of each of the functors h_A or h^A determines A up to isomorphism. It turns out that proving this result for h_A implies it for h^A, and vice-versa. See Exercise 30. Thus, we will only consider here the functor h_A.

Lemma 10.0.1 (Yoneda). *Let $F\colon \mathbf{C} \to \mathbf{Sets}$ be a covariant functor. Let $\mathrm{Mor}(h_A, F)$ denote the natural transformations from h_A to F.*

(1) There is a natural bijection

$$\mathrm{Mor}(h_A, F) \leftrightarrow F(A).$$

(2) $h_A \cong h_B$ if and only if $A \cong B$.

Proof. Let $\varphi\colon h_A \to F$ be a natural transformation. So for all $g\colon B \to C$ we have a commutative diagram

$$\begin{tikzcd} h_A(B) \arrow[r, "\varphi_B"] \arrow[d, "h_A(g)"] & F(B) \arrow[d, "F(g)"] \\ h_A(C) \arrow[r, "\varphi_C"] & F(C) \end{tikzcd}$$

where, of course, $h_A(g)(f) = g \circ f$. In particular, we have a function,

$$\varphi_A\colon h_A(A) \to F(A),$$

and we get a map $\mathrm{Mor}(h_A, F) \to F(A)$ by the rule

$$\varphi \mapsto \varphi_A(Id_A) =: u_\varphi.$$

Now, given any object B of $\mathbf{C}$ and $f\colon A \to B$, we have the following commutative diagram:

$$\begin{tikzcd}
h_A(A) \arrow[rrr, "\varphi_A"] \arrow[ddd, "h_A(f)"'] & & & F(A) \arrow[ddd, "F(f)"] \\
& Id_A \arrow[r, mapsto] \arrow[d, mapsto] & u_\varphi \arrow[d, mapsto] & \\
& f \arrow[r, mapsto] & \varphi_B(f) & \\
h_A(B) \arrow[rrr, "\varphi_B"'] & & & F(B)
\end{tikzcd}$$

This implies that

$$\varphi_B(f) = F(f)(u_\varphi).$$

Therefore, φ is determined by u_φ, and so we got an injective map

$$\mathrm{Mor}(h_A, F) \hookrightarrow F(A).$$

Conversely, given an element $u \in F(A)$, define for every $B \in \mathrm{Ob}(\mathbf{C})$ and any $f\colon A \to B$,

$$\varphi_B(f) := F(f)(u).$$

Note that φ_B is a function $h_A(B) \to F(B)$. Verifying it is a natural transformation amounts to check the commutativity of the following diagram for $g\colon B \to C$:

$$\begin{tikzcd}
h_A(B) \arrow[r, "\varphi_B"] \arrow[d, "h_A(g)"] & F(B) \arrow[d, "F(g)"] \\
h_A(C) \arrow[r, "\varphi_C"] & F(C)
\end{tikzcd}$$

Let $f\colon A \to B$. Then, on the one hand

$$F(g)(\varphi_B(f)) = F(g)(F(f)(u)) = F(g \circ f)(u),$$

while, on the other hand,

$$\varphi_C(h_A(g)(f)) = \varphi_C(g \circ f) = F(g \circ f)(u),$$

and so the diagram is commutative.

We now prove the second part of Yoneda's lemma. Let us first see what the first part gives for $F = h_B$. We proved

$$\mathrm{Mor}(h_A, h_B) \cong h_B(A) = \mathrm{Mor}(B, A).$$

And, in fact, the proof associated to $f\colon B \to A$ the natural transformation

$$\varphi^f : h_A \to h_B,$$

given by

$$\varphi^f_C : h_A(C) = \mathrm{Mor}(A, C) \to \mathrm{Mor}(B, C) = h_B(C), \qquad g \mapsto g \circ f.$$

From this, it is clear that a composition $B \xrightarrow{f_1} A \xrightarrow{f_2} B$ gives the relation

$$\varphi^{f_2 \circ f_1} = \varphi^{f_1} \circ \varphi^{f_2},$$

where $\varphi^{f_2 \circ f_1} \in \mathrm{Mor}(h_B, h_B)$, $\varphi^{f_2} \in \mathrm{Mor}(h_B, h_A)$, $\varphi^{f_1} \in \mathrm{Mor}(h_A, h_B)$. Also clear is that if $f_2 \circ f_1 = Id_B$ then $\varphi^{f_1} \circ \varphi^{f_2} = \varphi^{f_2 \circ f_1} = \varphi^{Id_B}$ is the identity transformation $h_B \to h_B$. And, the same way, if $f_1 \circ f_2 = Id_A$ then $\varphi^{f_2} \circ \varphi^{f_1}$ is the identity transformation $h_A \to h_A$. We conclude that if $A \cong B$ then $h_A \cong h_B$.

Conversely, given $\varphi\colon h_A \to h_B$ we have

$$\varphi_A\colon h_A(A) \to h_B(A),$$

and we have let

$$f := \varphi_A(Id_A) \in \mathrm{Mor}(B, A).$$

If we have morphisms $h_A \xrightarrow{\varphi} h_B \xrightarrow{\psi} h_A$ then the composition $\psi \circ \varphi\colon h_A \to h_A$ produces the map $(\psi \circ \varphi)_A(Id_A)$ from A to A.

Claim. We have

$$(\psi \circ \varphi)(Id_A) = \varphi_A(Id_A) \circ \psi_B(Id_B).$$

Proof. Let us denote $f = \varphi_A(Id_A)\colon B \to A, g = \psi_B(Id_B)\colon A \to B$. Consider the following commutative diagram

$$\begin{tikzcd}
h_A(A) \arrow[r, "\varphi_A"] \arrow[rr, bend left, "(\psi\circ\varphi)_A"] & h_B(A) \arrow[r, "\psi_A"] & h_A(A) \\
& h_B(B) \arrow[u, "h_B(f)"] \arrow[r, "\psi_B"] & h_A(B) \arrow[u, "h_A(f)"']
\end{tikzcd}$$

We have,

$$\begin{aligned}
(\psi \circ \varphi)_A(Id_A) &= \psi_A(\varphi_A(Id_A)) \\
&= \psi_A(f) \\
&= \psi_A(h_B(f)(Id_B)) \\
&= h_A(f)(\psi_B(Id_B)) \\
&= h_A(f)(g) \\
&= f \circ g.
\end{aligned}$$

This proves the claim. □

Now, if $\psi \circ \varphi$ is the identity transformation $h_A \to h_A$ then clearly $(\psi \circ \varphi)_A(Id_A) = Id_A$ and so $f \circ g = Id_A$. A similar argument gives that if $\varphi \circ \psi$ is the identity transformation $h_B \to h_B$ then $g \circ f = Id_B$. We conclude that if $h_A \cong h_B$ then $A \cong B$. □

A covariant (resp. contravariant) functor $G\colon \mathbf{C} \to \mathbf{Sets}$ is called **representable** if there is $X \in \mathrm{Ob}(\mathbf{C})$ such that $G \cong h_X$ (resp. $G \cong h^X$). Yoneda's lemma shows that if G is representable, X is determined up to isomorphism. This issue comes up when one considers moduli problems. Unfortunately, I do not know any simple example of a moduli space, but consider the following.

Let G be a group. We usually consider complex reprenesentations of G, but now fix an integer $n \geq 1$ and given any commutative ring R consider homomorphisms $\rho\colon G \to GL_n(R)$. Given $\rho_i\colon G \to \mathrm{GL}_n(R)$, $i = 1, 2$, we consider them isomorphic if there is a matrix in $\mathrm{GL}_n(R)$ conjugating one representation into the other. The covariant functor F sending a ring R into the set of representations $\rho\colon G \to GL_n(R)$ is representable by a $\mathbb{Z}$-algebra. It is a quotient of the free polynomial ring $R^{univ} := \mathbb{Z}[x_{ij}^g : g \in G, 1 \leq i, j \leq n]$ by the ideal expressing the conditions

$$(x_{ij}^g)(x_{ij}^h) = (x_{ij}^{gh}).$$

To give $\rho\colon G \to GL_n(R)$ is to give a homomorphism $R^{univ} \to R$. And so $h_{R^{univ}}$ represents F.

However, what we are really interested in is studying representations up to isomorphism. This turns out to be a subtle problem; in a sense, one would like to take the invariants of R^{univ}

under the action of $\mathrm{PGL}_n(R^{univ})$ acting by conjugation. This doesn't quite work, but it turns out that there is a variant that does. Suppose we only want to consider geometrically irreducible representations of G. Namely, such $\rho\colon G \to GL_n(R)$ with the property that for every prime ideal $\mathfrak{p}$ of R and an algebraically closed field $k \supset R/\mathfrak{p}$ the composite representation

$$G \to \mathrm{GL}_n(R) \to GL_n(R/\mathfrak{p}) \to GL_n(k)$$

is irreducible. Associating to R the set of isomorphism classes of geometrically irreducible n-dimensional representations $\rho\colon G \to \mathrm{GL}_n(R)$ is a functor G, which turns out to be representable. This is a non-trivial result proved only in 2000 by Nakamoto.

Here is why one might be interested. Consider a compact Riemann surface X of genus g. The isomorphism classes of vector bundles with flat connection on X are in correspondence with isomorphism classes of representations

$$\pi_1(X, x_0) \to \mathrm{GL}_n(\mathbb{C}).$$

In particular, line bundles of degree 0 (that are automatically endowed with a flat connection) are in bijection with homomorphisms

$$\pi_1(X, x_0) \to \mathbb{C}^*.$$

Equivalently, with homomorphisms

$$\mathbb{Z}^{2g} = H_1(X, \mathbb{Z}) \to \mathbb{C}^*.$$

These are in bijection with $(\mathbb{C}^\times)^{2g}$ by associating to a homomorphism $f\colon \mathbb{Z}^{2g} \to \mathbb{C}^*$ the vector $(f(e_1), \dots, f(e_{2g})) \in (\mathbb{C}^\times)^{2g}$.

Given a family of line bundles with connection over X that is parameterized by $\mathbb{P}^1$, we get an analytic map

$$\mathbb{P}^1 \to (\mathbb{C}^\times)^{2g}.$$

(The fact that we get an analytic map requires some work and rests on the fact that the functor G is representable.) By the maximum principle, this map must be constant. Thus, a family of line bundles on X that is parameterized by $\mathbb{P}^1$ is in fact constant.

Returning to simpler, but somewhat less exciting, examples consider a forgetful functor

$$\Phi : \mathbf{C} \to \mathbf{Sets}.$$

Here is it assumed that the objects of C are in particular sets and so $\Phi(B)$ is B considered as a set only. For example, $\mathbf{C}$ could be the category of groups and $\Phi(B)$ is "forgetting that B is a group and considering it as a set only". Often these functors have a right adjoint functor G which is a "free construction functor". That is, we have

$$\mathrm{Mor}_{\mathbf{C}}(G(A), B) \cong \mathrm{Mor}_{\mathbf{Sets}}(A, \Phi(B)).$$

Now, if we take $A = \{a\}$ a singleton. Then $\mathrm{Mor}_{\mathbf{Sets}}(A, \Phi(B))$ is identified with $\Phi(B)$. On the other hand, we have $\mathrm{Mor}_{\mathbf{C}}(G(\{a\}), B) \cong \mathrm{Mor}_{\mathbf{Sets}}(A, \Phi(B))$. Thus, we get that the functor Φ is representable by h_X, where $X = G(\{a\})$. In the example of the category of groups $G(\{a\}) \cong \mathbb{Z}$ and we conclude that as sets we have natural bijections

$$\mathrm{Hom}_{\mathbf{Grps}}(\mathbb{Z}, B) \leftrightarrow B.$$

11. Equivalence of categories

In this section we will prove two theorems. The first is a general criterion for a functor to be an equivalence of categories. The second, is a particular example of equivalence of categories, called Morita equivalence, that is very useful in applications.

11.1. **Criterion for a functor to be an equivalence of categories.**

Let $\mathbf{C}, \mathbf{D}$ be categories and $F\colon \mathbf{C} \to \mathbf{D}$ a covariant functor. Recall that F is called *faithful* if for any $A, B \in \mathrm{Ob}(\mathbf{C})$ the map

$$\mathrm{Mor}_{\mathbf{C}}(A,B) \to \mathrm{Mor}_{\mathbf{D}}(F(A), F(B)),$$

is injective; it is called *full*, if this map is surjective. We say F is **essentially surjective**, if any object of $\mathbf{D}$ is isomorphic to some $F(A)$, where A is an object of $\mathbf{C}$.

Theorem 11.1.1. *Let $F\colon \mathbf{C} \to \mathbf{D}$ be a covariant functor. There exists a functor $G\colon \mathbf{D} \to \mathbf{C}$ such that (F, G) is an equivalence of categories if and only if:*

(1) F is full and faithful;
(2) F is essentially surjective.

Proof. It will be useful to recall the following. Suppose that $L\colon \mathbf{C} \to \mathbf{C}$ is a covariant functor and

$$\gamma\colon \mathbb{1}_{\mathbf{C}} \overset{\sim}{\to} L$$

is a natural equivalence. Then, for all objects A, B, and morphisms $f\colon A \to B$, we have a commutative diagram:

$$\begin{tikzcd}
A \arrow[r, "\gamma_A", "\sim"'] \arrow[d, "f"'] & L(A) \arrow[d, "L(f)"] \\
B \arrow[r, "\gamma_B", "\sim"'] & L(B)
\end{tikzcd}$$

and so,

$$L(f) = \gamma_B \circ f \circ \gamma_A^{-1}$$

and $f \mapsto L(f)$ is therefore an isomorphism

$$\mathrm{Mor}(A,B) \overset{\sim}{\longrightarrow} \mathrm{Mor}(L(A), L(B)).$$

Back to the theorem, suppose that a covariant functor $G\colon \mathbf{D} \to \mathbf{C}$ exists with isomorphisms

$$\gamma\colon \mathbb{1}_{\mathbf{C}} \overset{\sim}{\longrightarrow} GF, \qquad \delta\colon \mathbb{1}_{\mathbf{D}} \overset{\sim}{\longrightarrow} FG.$$

We have the diagram

$$\begin{tikzcd}
A \arrow[rrrr, bend left, "\gamma_A", "\cong"'] \arrow[dd, "f"'] & & F(A) \arrow[dd, "F(f)"'] & & GF(A) \arrow[dd, "GF(f)"'] \\
 & \sim> & & \sim> & \\
B \arrow[rrrr, bend right, "\gamma_B"'] & & F(B) & & GF(B)
\end{tikzcd}$$

$$\cong$$

As $f \mapsto GF(f)$ is an isomorphism that factors through $f \mapsto F(f)$, $f \mapsto F(f)$ must be injective. That is, F is faithful. By symmetry, G is faithful, too.

Now, given $h\colon F(A) \to F(B)$, let $f\colon A \to B$ be defined by

$$f = \gamma_B^{-1} \circ G(h) \circ \gamma_A.$$

Since G is faithful, to show that $F(f) = h$ it is enough to prove that $GF(f) = G(h)$ and this is clear: $GF(f) = \gamma_B \circ f \circ \gamma_A^{-1} = G(h)$. We conclude that F is full.

Let D be an object of $\mathbf{D}$ and let $C = G(D)$. Then, we have an isomorphism

$$\delta_D\colon D \to FG(D) = F(C),$$

and it follows that F is essentially surjective.

Conversely, let F be a fully-faithful essentially surjective covariant functor $\mathbf{C} \to \mathbf{D}$. To define

$$G\colon \mathbf{D} \to \mathbf{C}$$

first choose, in an arbitrary fashion, for any object D of $\mathbf{D}$ an object C_D of $\mathbf{C}$ and an isomorphism

$$\eta_D\colon D \to F(C_D).$$

Define G on objects by

$$G(D) = C_D.$$

Define G on morphisms by the following diagram:

$$\begin{tikzcd}
D \arrow[r, "\eta_D"] \arrow[dd, "g"'] & F(C_D) \arrow[dd, "g'"] & & & C_D \arrow[dd, "f"] \\
& & {} & {} \arrow[l, squiggly, "F"] & \\
E \arrow[r, "\eta_E"] & F(C_E) & & & C_E
\end{tikzcd}$$

(where g' is uniquely determined). Namely, there is a unique $f\colon C_D \to C_E$ such that $F(f) = g'$. We let $G(g) = f$. Otherwise said,

for $g\colon D \to E$, $G(g)$ is the unique morphism $C_D \to C_E$ such that

$$F(G(g)) = g' := \eta_E \circ g \circ \eta_D^{-1}.$$

There is much to check. Firstly, that G is a functor:

(1) $G(1_D) = 1_{C_D}$. This holds because $F(1_{C_D}) = 1_{F(C_D)} = \eta_D \circ 1_D \circ \eta_D^{-1}$.

(2) $G(g_2 \circ g_1) = G(g_2) \circ G(g_1)$. The situation is explained by the following diagram

$$\begin{tikzcd}
D_1 \arrow[r, "\eta_{D_1}"] \arrow[dd, "g_1"'] & F(C_{D_1}) \arrow[dd, "g_1'"] & & & C_{D_1} \arrow[dd, "G(g_1)"] \\
& & {} & {} \arrow[l, squiggly, "F"] & \\
D_2 \arrow[r, "\eta_{D_2}"] \arrow[dd, "g_2"] & F(C_{D_2}) \arrow[dd, "g_2'"] & & & C_{D_2} \arrow[dd, "G(g_2)"] \\
& & {} & {} \arrow[l, squiggly, "F"] & \\
D_3 \arrow[r, "\eta_{D_3}"] & F(C_{D_3}) & & & C_{D_3}
\end{tikzcd}$$

The commutativity of the squares gives

$$g_2' \circ g_1' = (g_2 \circ g_1)'.$$

Also,

$$F(G(g_2) \circ G(g_1)) = FG(g_2) \circ FG(g_1) = g_2' \circ g_1' = (g_2 \circ g_1)',$$

which, by the property characterizing $G(g_2 \circ g_1)$, implies

$$G(g_2) \circ G(g_1) = G(g_2 \circ g_1).$$

Thus, G is a functor. We next need to define isomorphisms

$$\gamma\colon \mathbb{1}_{\mathbf{C}} \to GF, \quad \delta\colon \mathbb{1}_{\mathbf{D}} \to FG.$$

We begin with γ. Let C be an object of $\mathbf{C}$ and $D = F(C)$. We have chosen an isomorphism $\eta_D\colon D = F(C) \to F(C_D)$, which comes by full-faithfulness from a unique isomorphism

$$\gamma_C\colon C \to C_D = G(D) = GF(C).$$

That is, we let $\gamma_C\colon C \to GF(C)$ be the unique isomorphism such that $F(\gamma_C) = \eta_D$. Having defined the isomorphisms γ_C, we need to check that the following diagram commutes for every $h\colon C_1 \to C_2$:

$$\begin{tikzcd}
C_1 \arrow[r, "\gamma_{C_1}"] \arrow[d, "h"] & GF(C_1) \arrow[d, "GF(h)"] \\
C_2 \arrow[r, "\gamma_{C_2}"] & GF(C_2)
\end{tikzcd}$$

Since F is faithful, it is enough to check commutativity after applying F to the diagram and that yields:

$$\begin{tikzcd}
D_1 := F(C_1) \arrow[r, "\eta_{D_1}"] \arrow[d, "F(h)"] & F(C_{D_1}) \arrow[d, "FGF(h)"] \\
D_2 := F(C_2) \arrow[r, "\eta_{D_2}"] & F(C_{D_2})
\end{tikzcd}$$

(recall that $GF(C_1) = C_{F(C_1)} = C_{D_1}$ and so $FGF(C_1) = F(C_{D_1})$.) If we let $t = F(h)$ then $G(t)$ is the morphism $C_{D_1} \to C_{D_2}$ such that $FG(t) = \eta_{D_2} \circ t \circ \eta_{D_1}^{-1}$. So commutativity follows.

Next, δ. Given D an object of $\mathbf{D}$ we want to define an isomorphism

$$\delta_D\colon D \to FG(D) = F(C_D).$$

But, we have already chosen one: η_D. So we let

$$\delta_D = \eta_D.$$

For $f\colon D_1 \to D_2$, we need to check commutativity of the diagram:

$$\begin{tikzcd}
D_1 \arrow[r, "\delta_{D_1}"] \arrow[dd, "f"] & FG(D_1) \arrow[dd, "FG(f)"] & & & G(D_1) = C_{D_1} \arrow[dd, "G(f)"] \\
& & {} & {} \arrow[l, squiggly, "F"'] & \\
D_2 \arrow[r, "\delta_{D_2}"] & FG(D_2) & & & G(D_2) = C_{D_2}
\end{tikzcd}$$

But this is precisely the definition of $G(f)$. □

A common application of this theorem is finding a small set of representatives for a very big category. Suppose $\mathbf{D}$ is a category and $\mathbf{C}$ is a **full subcategory** of $\mathbf{D}$. That is, the objects of $\mathbf{C}$ are objects of $\mathbf{D}$ and $\mathrm{Mor}_{\mathbf{C}}(A, B) = \mathrm{Mor}_{\mathbf{D}}(A, B)$ for objects of $\mathbf{C}$. If every object of $\mathbf{D}$ is isomorphic to some object of $\mathbf{C}$ then the categories $\mathbf{C}$ and $\mathbf{D}$ are equivalent.

For example, if **D** is the category of finitely generated abelian groups, we can take **C** to be the subcategory whose objects are abelian groups of the form $\mathbb{Z}^r \oplus \oplus_{i=1}^n (\mathbb{Z}/d_i\mathbb{Z})$ where $1 < d_1|d_2|\cdots|d_n$ (and $r, n \geq 0$).

11.2. **Morita equivalence.** Let R be a ring, not necessarily commutative. Then $M_n(R)$ is also a ring under the usual matrix operation, only that one has to be very methodic keeping right right and left left. Namely,

$$(a_{ij})(b_{ij}) = (c_{ij}),$$

where

$$c_{ij} = \sum_\ell a_{i\ell}b_{\ell j},$$

which might be different than $\sum_\ell b_{\ell j}a_{i\ell}$. We view R as contained in $M_n(R)$ via

$$R \to M_n(R), \quad r \mapsto r \cdot I_n.$$

Denote by E_{ij} the $n \times n$ matrix all whose entries are zero, except the ij entry which is 1. These matrices have two important properties:

- for $r \in R$ we have $rE_{ij} = E_{ij}r$;
- $E_{\ell k}E_{ij} = \delta_{ki}E_{\ell j}$, where δ_{ki} is Kronecker's delta function.

As an application of our criterion for equivalence of categories, we prove the following theorem, which is part of what's called **Morita equivalence**.

Theorem 11.2.1 (Morita). *Let R be a ring and $n \geq 1$ an integer. The categories ${}_{\mathbf{R}}\mathbf{Mod}$ and ${}_{\mathbf{M_n(R)}}\mathbf{Mod}$ are equivalent.*

Proof. Define

$$F\colon {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{M_n(R)}}\mathbf{Mod}$$

by

$$F(M) = M^n$$

on objects and

$$F(f) = {}^t(f, f, \dots, f),$$

for a morphism $f\colon M \to N$. Here we think about M^n as columns vectors with entries in M and denote an element $(m_1, \dots, m_n)$ of it by $\underline{m}$. The action of $M_n(R)$ is given by the usual formula

$$(a_{ij})_{i,j=1}^n \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \sum_\ell a_{1\ell}m_\ell \\ \vdots \\ \sum_\ell a_{n\ell}m_\ell \end{pmatrix}.$$

It is obvious that F is a faithful functor.

Now, any morphism $\varphi\colon M^n \to N^n$ of $M_n(R)$ modules is of the form

$$\varphi(\underline{m}) = {}^t(\varphi_1(\underline{m}), \dots, \varphi_n(\underline{m})),$$

and the φ_i are maps of R-modules. We therefore have

$$\varphi({}^t(m, 0, \dots, 0)) = \varphi(E_{11}{}^t(m, 0, \dots, 0)) = E_{11}\varphi({}^t(m, 0, \dots, 0)) = {}^t(\varphi_1(m, 0, \dots, 0), 0, \dots, 0).$$

This implies that φ_i vanishes on ${}^t(m, 0, \dots, 0)$ for all $i \neq 1$. Similarly, we conclude that φ_i vanishes on ${}^t(0, \dots, 0, \underset{j}{m}, 0, \dots, 0)$ for any $i \neq j$. Using additivity of φ, it follows that

$$\varphi({}^t(m_1, \dots, m_n)) = (\varphi_1(m_1), \dots, \varphi_n(m_n)).$$

Let $\sigma \in S_n$ and $E(\sigma)$ the matrix $\rho^{St}(\sigma^{-1})$ so that

$$E(\sigma)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} m_{\sigma(1)} \\ \vdots \\ m_{\sigma(n)} \end{pmatrix}.$$

Then, on the one hand

$$\varphi(E(\sigma)^t(m_1, \dots, m_n)) = {}^t(\varphi_1(m_{\sigma(1)}), \dots, \varphi_n(m_{\sigma(n)})),$$

On the other hand,

$$\varphi(E(\sigma)^t(m_1, \dots, m_n)) = E(\sigma)\varphi({}^t(m_1, \dots, m_n)) = (\varphi_{\sigma(1)}(m_{\sigma(1)}), \dots, \varphi_{\sigma(n)}(m_{\sigma(n)}).$$

As this holds for all σ and every $m_i \in M$, we conclude that

$$\varphi_1 = \cdots = \varphi_n.$$

That is,

$$\varphi = F(\varphi_1),$$

and F is a full functor.

It remains to prove that F is essentially surjective and this is the most subtle part. Let M be an $M_n(R)$ module.

Claim 1. We have an isomorphism of left R-modules

$$M \cong E_{11} \cdot M \oplus \cdots \oplus E_{nn} \cdot M.$$

To prove that consider the functions

$$f\colon M \to E_{11} \cdot M \oplus \cdots \oplus E_{nn} \cdot M, \quad m \mapsto (E_{11}m, \dots, E_{nn}m)$$

and

$$g\colon E_{11} \cdot M \oplus \cdots \oplus E_{nn} \cdot M \to M, \quad (a_1, \dots, a_n) \mapsto a_1 + \cdots + a_n.$$

These maps are homomorphisms of R-modules and are mutual inverses. We have

$$g(f(m)) = \sum_i E_{ii} \cdot m = (\sum_i E_{ii}) \cdot m = 1 \cdot m = m.$$

Writing $a_i = E_{ii}a'_i$ we find that

$$\begin{aligned} f(g(a_1, \dots, a_n)) &= (E_{11} \cdot (\sum_j E_{jj}a'_j), \dots, E_{nn} \cdot (\sum_j E_{jj}a'_j)) \\ &= (\sum_j E_{11}E_{jj}a'_j, \dots, \sum_j E_{nn}E_{jj}a'_j) \\ &= (E_{11}a'_1, \dots, E_{nn}a'_n) \\ &= (a_1, \dots, a_n). \end{aligned}$$

Claim 2. We have equalities $E_{\ell 1}M = E_{\ell\ell}M$.

Indeed, as $E_{\ell 1} = E_{\ell\ell}E_{\ell 1}$, we have $E_{\ell 1}M = E_{\ell\ell}(E_{\ell 1}M) \subseteq E_{\ell\ell}M$. On the other hand, as $E_{\ell\ell} = E_{\ell 1}E_{1\ell}$, we have $E_{\ell\ell}M = E_{\ell 1}(E_{1\ell}M) \subseteq E_{\ell 1}M$.

We thus conclude that

$$E_{11}M \oplus \cdots \oplus E_{n1}M \cong M, \quad (a_1, \dots, a_n) \mapsto \sum a_i.$$

Claim 3. We have isomorphisms $E_{11}M \cong E_{\ell 1}M$ by the map $a \overset{f}{\mapsto} E_{\ell 1}a$.

The map $a \mapsto E_{\ell 1}a$ is restriction of the R-module homomorphism $M \to E_{\ell 1}M$ given by the same formula. Therefore, it is an R-module homomorphism. We claim that the map

$$E_{\ell 1}M \to E_{11}M, \quad b \overset{g}{\mapsto} E_{1\ell}b,$$

is a well-defined inverse map. Let us write $a = E_{11}a' \in E_{11}M, b = E_{\ell 1}b' \in E_{\ell 1}M$. We first note that $g(b) = E_{1\ell}E_{\ell 1}b' = E_{11}b' \in E_{11}M$ and so g is well-defined. Now,

$$g(f(a)) = g(f(E_{11}a')) = E_{1\ell}E_{\ell 1}E_{11}a' = E_{11}a' = a.$$

Also,

$$f(g(b)) = E_{\ell 1}E_{1\ell}E_{\ell 1}b' = E_{\ell 1}b' = b.$$

Collecting the three claims together, we conclude that we have an isomorphism

$$\varphi : F(E_{11}M) = E_{11}M \oplus \cdots \oplus E_{11}M \to M,$$

given by the map

$$(a_1, \dots, a_n) \mapsto (E_{11}a_1, \dots, E_{n1}a_n) \mapsto \sum_{\ell=1}^{n} E_{\ell 1}a_\ell.$$

But this is so far an isomorphism of R-modules. We have to check that this isomorphism is an isomorphism of $M_n(R)$ modules. As $M_n(R)$ is spanned over R by the matrices E_{ij} and $(E_{11}M)^n$ is spanned over R by vectors of the form ${}^t(0, \dots, 0, a, 0, \dots, 0)$, it is enough to check that

$$\varphi(E_{\ell k}{}^t(0, \dots, 0, a, 0, \dots, 0)) = E_{\ell k}\varphi({}^t(0, \dots, 0, a, 0, \dots, 0)),$$

where a is at the i-th coordinate.

If $i \neq k$ then $E_{\ell k}{}^t(0, \dots, 0, a, 0, \dots, 0) = 0$ and so $\varphi(E_{\ell k}{}^t(0, \dots, 0, a, 0, \dots, 0)) = 0$. Also, $\varphi({}^t(0, \dots, 0, a, 0, \dots, 0)) = E_{i1}a$ and so $E_{\ell k}\varphi({}^t(0, \dots, 0, a, 0, \dots, 0)) = E_{\ell k}E_{i1}a = 0$.

If $i = k$ then $\varphi(E_{\ell i}{}^t(0, \dots, 0, \underset{i}{a}, 0, \dots, 0)) = \varphi({}^t(0, \dots, 0, \underset{\ell}{a}, 0, \dots, 0)) = E_{\ell 1}a$, and on the other hand, $E_{\ell i}\varphi({}^t(0, \dots, 0, a, 0, \dots, 0)) = E_{\ell i}E_{i1}a = E_{\ell 1}a$. □

11.2.1. *Division algebras.* A classical application of this equivalence is when one can completely classify the R-modules. You can amuse yourself by considering finitely generated $\mathbb{Z}$-modules. We will discuss an extreme case when R is a division ring. Recall that a **division ring**, or a **skew field** is a ring R in which $0 \neq 1$ and every non-zero element is a unit of R. That is, if $x \neq 0$ is an element of R then there exists $y \in R$ such that $xy = yx = 1$. The simplest example is a field, of course.

If R is a division ring then the centre of R is a field and R is an algebra over it. It thus makes sense to already discuss division algebras R over a field K, meaning that R is a division ring containing K in its centre. The problem of classification of division algebras over a field K is a complicated and difficult one. Assume that R is of finite dimension over K. Here are some interesting results:

- If K is a finite field then R is a finite field as well. (A theorem of Wedderburn. See proof below.).
- If R is the real numbers, R is either $\mathbb{R}, \mathbb{C}$ or the **Hamilton quaternions**
$$\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$
with $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$. In particular, there are no division algebras whose dimension over $\mathbb{C}$ is 9, say.
- Suppose that the characteristic of K is not 2. There is then a general construction of 4-dimensional K-algebras called **quaternion algebra**. Let $a, b \in K^\times$ and define an algebra R, often denoted $\left(\frac{a,b}{k}\right)$, by
$$K \oplus Ki \oplus Kj \oplus Kk,$$

where $i^2 = a, j^2 = b, ij = -ji = k$. Define the **norm** of an element $u = x + yi + zj + wk$, $x, y, z, w \in K$, of R by

$$N(u) = N(x + yi + zj + wk) = x^2 - ay^2 - bz^2 + abw^2.$$

We have the following properties of the norm function:
(1) $N(u) = u\bar{u}$, where $\bar{u} = x - yi - zj - wk$;
(2) $N(u_1u_2) = N(u_1)N(u_2)$.
Using this, it is not hard to prove that u is invertible if and only if $N(u) \neq 0$. Thus, R is a division algebra if and only if the quadratic form $x^2 - ay^2 - bz^2 + abw^2$ does not represent 0 (this means that the only solution to $x^2 - ay^2 - bz^2 + abw^2 = 0$ is $x = y = z = w = 0$). For example, if $K = \mathbb{R}$ and $a = b = -1$ we get the form $x^2 + y^2 + z^2 + w^2$ and conclude that the Hamilton quaternions are indeed a division algebra. For more on this topic, see Exercise 34.

- Over $\mathbb{Q}$ there are "plenty" of non-isomorphic non-commutative division algebras. For example, for every positive integer n there is a division algebra whose centre is precisely $\mathbb{Q}$ and whose dimension over $\mathbb{Q}$ is n^2. A more general notion is that of a central simple algebra over $\mathbb{Q}$, or a field K. It turns out that there is a group whose elements are central simple algebras R over K, up to an equivalence $R \sim M_n(R)$ for every n. It is called the **Brauer group**. In this group every quaternion algebra over R has order equal to 2, unless it is isomorphic to $M_2(K)$, in which case it has order 1. The group structure if given by the tensor product over K.

If R is a division algebra the theory of R-modules is rather similar to the theory of vector spaces initially. Things go wrong once we get to determinants, eigenvectors, eigenvalues, due to the non-commutativity of R, but initially there is hardly a difference. The definition of linearly independent sets, spanning sets and so on, are the same. There are the same characterizations of a basis and Steinitz substitution lemma works and provides the invariance of dimension. It requires nothing but patience to prove that every finitely generated R-module is isomorphic to R^d for some integer $d \geq 0$ that is uniquely determined. Morita equivalence now gives that every finitely generated $M_n(R)$-module is of the form $(R^d)^n$ for some d. Otherwise said, every $M_n(R)$-module is isomorphic to a direct sum of R^n, where R^n is viewed as column vectors of length n with entries in R.

11.2.2. *Proof of Wedderburn's little theorem.*

Theorem 11.2.2 (Wedderburn)**.** *Let R be a finite division ring then R is a field.*

Proof. (E. Witt) Let R be a finite division ring. We prove the theorem by induction on the cardinality of R; the case $|R| = 2$ is clear.

Let K be the centre of R. It is a field with q elements. Let $n = \dim_K(R)$. Our goal is to prove that $n = 1$. Suppose that $n > 1$. Let $r \in R \setminus K$ and let K_r be its centralizer in R. It is easy to check that K_r is a division algebra as well and that we have inclusions

$$K \subseteq K_r \subsetneqq R.$$

Thus, using induction, K_r is a field too. If we let $n_r = \dim_K(K_r)$ we have $n_r | n$ and $1 \leq n_r < n$. The multiplicative groups $K^\times, K_r^\times, R^\times$, have orders $q - 1, q^{n_r} - 1, q^n - 1$, respectively.

Write the class equation for the multiplicative group $R^\times$ acting on itself by conjugation:

$$q^n - 1 = q - 1 + \sum_{r \notin K} \frac{q^n - 1}{q^{n_r} - 1},$$

where the summation is over representatives for the conjugacy classes of elements $r \notin K$.

The idea now is to find an integer dividing $\frac{q^n-1}{q^{n_r}-1}$ for all r and therefore $q-1$. We will show that this integer is larger than $q-1$, thereby arriving at a contradiction.

For a positive integer b, let $\Phi_b(x) = \prod_{\zeta \text{ prim. root of order } b}(x-\zeta) \in \mathbb{Z}[x]$ denote the (monic) cyclotomic polynomial of degree $\varphi(b)$ (where φ is Euler's function). Then

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \qquad x^{n_r} - 1 = \prod_{d|n_r} \Phi_d(x).$$

As $n_r|n$ we have $\Phi_n(x)|\frac{x^n-1}{x^{n_r}-1}$. Substituting q for x, we find that

$$\Phi_n(q)|\frac{q^n-1}{q^{n_r}-1}.$$

By the class equation, the integer $\Phi_n(q)$ divides $q-1$ as well. On the other hand

$$\Phi_n(q) = \prod_{\zeta}(q-\zeta),$$

where the product is taken over all $\varphi(n)$ roots of unity of order n. As the absolute value of each such complex number $q-\zeta$ is greater than $q-1$ we find $|\Phi_n(q)| > q-1$. Contradiction. □

12. Universal property

We begin with a few examples where one would use the terminology "universal property" and then examine what is exactly meant by that.

Example 12.0.1. (Abelianization) Let G be a group and $G^{ab} = G/G'$ its abelianization. One says that G^{ab} has the following universal property: *Any homomorphism $f\colon G \to A$ from G to an abelian group A factors uniquely as*

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "f"'] & G^{ab} \arrow[d] \\ & A \end{tikzcd}$$

Example 12.0.2. (Direct product) Let G_1, G_2 be groups. The group $G_1 \times G_2$ has the following universal property. There are group homomorphisms, the projections on the i-th coordinate, $p_i\colon G_1 \times G_2 \to G_1$, $p_i(g_1, g_2) = g_i$, such that given any group H and homomorphisms $q_i\colon H \to G_i$, there is a unique homomorphism $f\colon H \to G_1 \times G_2$ such that the following diagram commutes:

$$\begin{tikzcd} & H \arrow[d, "f"] \arrow[ddl, "q_1"'] \arrow[ddr, "q_2"] & \\ & G_1 \times G_2 \arrow[dl, "p_1"] \arrow[dr, "p_2"'] & \\ G_1 & & G_2 \end{tikzcd}$$

Indeed, f must be (q_1, q_2).

Example 12.0.3. (Tensor product) Let R be a ring and M_R, ${}_RN$ two R-modules. Then the abelian group $M \otimes_R N$ has the following universal property: there is an R-biadditive map $M \times N \to M \otimes_R N$, $(m, n) \mapsto m \otimes n$, such that given any abelian group A and an R-biadditive map $M \times N \to A$, there is a unique group homomorphism $M \otimes_R N \to A$ making the following diagram commutative:

$$\begin{tikzcd}
M \times N \arrow[r] \arrow[dr] & M \otimes_R N \arrow[d] \\
 & A
\end{tikzcd}$$

We will now explain in which sense each of these examples can be phrased as the existence of an initial, or final, object in a category. For these notions, see Exercise 1.

In the first example (abelianization), define a category whose objects are homomorphisms $f\colon G \to A$ from G to abelian groups A and morphisms $h \in \mathrm{Mor}((f\colon G \to A), (g\colon G \to B))$ are commutative diagrams

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[dr, "g"'] & A \arrow[d, "h"] \\
 & B
\end{tikzcd}$$

Then $G \to G^{ab}$ is an initial object of this category.

In the second example (direct product), define a category whose objects are pairs of homomorphisms $\{q_i\colon H \to G_i\}_{i=1,2}$, where H is a group. Define a morphism in this category $h \in \mathrm{Mor}(\{q_i\colon H \to G_i\}, \{q_i'\colon H' \to G_i\})$ to be a homomorphism $h : H \to H'$ such that the following diagram commutes:

$$\begin{tikzcd}
 & H \arrow[d, "h"] \arrow[ddl, "q_1"'] \arrow[ddr, "q_2"] & \\
 & H' \arrow[dl, "q_1'"] \arrow[dr, "q_2'"'] & \\
G_1 & & G_2
\end{tikzcd}$$

Then $\{p_i : G_1 \times G_2 \to G_i\}$ is a final object of this category.

In the third example (tensor product), define a category whose objects are R-biadditive maps $f\colon M \times N \to A$ into abelian groups. A morphism h in the category, $h \in \mathrm{Mor}((f\colon M \times N \to A), (g\colon M \times N \to B))$, is a group homomorphism $h\colon A \to B$, such that the following diagram commutes

$$\begin{tikzcd}
M \times N \arrow[r, "f"] \arrow[dr, "g"'] & A \arrow[d, "h"] \\
 & B
\end{tikzcd}$$

Then $M \times N \to M \otimes_R N$ is an initial object in this category.

This is as much as we are going to say about the subject. Whenever we refer to a **universal property** implicit is that there is an associated category in which the situation we are talking about is an initial or final object of that category. In particular, *they are unique up to unique isomorphism*.

13. Limits

13.1. **Direct limits.** Imagine a diagram of objects and morphisms of a category **C**.

$$\begin{tikzcd}
 & X_1 \arrow[r, "f_{12}"] \arrow[dl, "f_{14}"'] \arrow[d] & X_2 \arrow[dll, "f_{24}"] \arrow[dr] \arrow[dd] & X_3 \arrow[d] \arrow[ddl] \\
X_4 & X_5 & & X_6 \arrow[dl] \\
 & X_7 \arrow[r] & X_8 &
\end{tikzcd}$$

To be precise, we assume that we are given a partially order set I and for every $i \in I$ an object X_i of **C**, for every $i \leq j$ a morphism $f_{i,j} \colon X_i \to X_j$ with $f_{ii} = 1_{X_i}$, and whenever $i \leq j \leq k$ we have $f_{ik} = f_{jk} \circ f_{ij}$. We call this is a **direct system** or **injective system**. A word of caution: often one uses this terminology under the further assumption that I is a **directed poset** (or, **directed index set**), meaning that for all $i, j \in I$ there is a $k \in I$ with $i \leq k$ and $j \leq k$. But we shall try and avoid this assumption to the extent possible. We will denote such a diagram

$$\{X_i, f_{ij}\}.$$

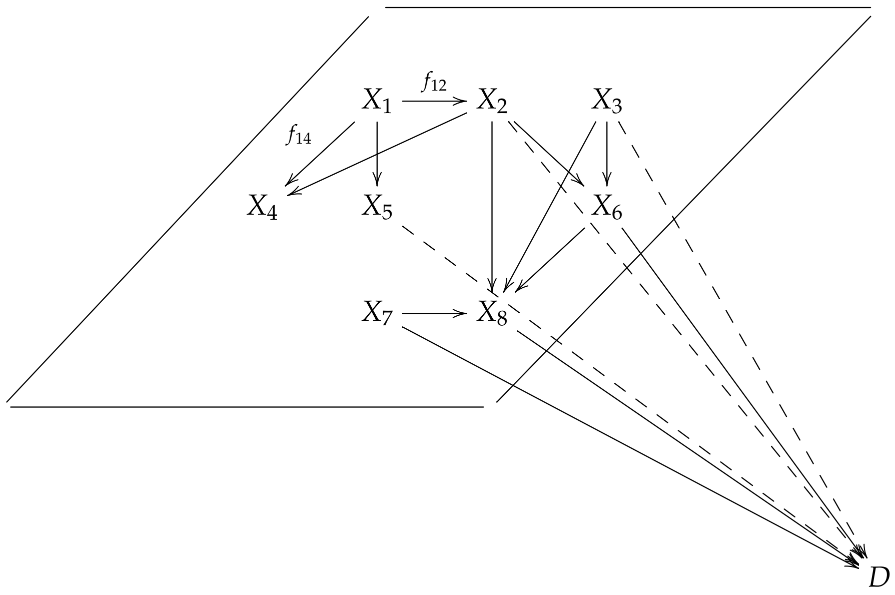
If we think about I as a category $\underline{I}$, whose objects are the elements of I and

$$\mathrm{Mor}(x, y) = \begin{cases} i_{xy} & x \leq y \\ \emptyset & else, \end{cases}$$

then a direct system corresponds to a covariant functor

$$\underline{I} \to \mathbf{C}.$$

We say that an object D of **C** is below the diagram in the following situation (the dashed arrows are morphisms too. We use dash lines to ease reading; also, there should be an arrow starting at every X_i, but we omit some arrows to keep the diagram easier to read):



and then the direct limit is an object of **C**, *if such exists*, that is closest to the diagram from below. More formally, the **direct limit**, or **injective limit** (again, be cautious that many authors use this terminology only if I is a directed index set and would use the terminology **colimit** instead) of $\{X_i, f_{ij}\}$ is an object C of **C**, together with morphisms

$$e_i : X_i \to C, \quad i \in I,$$

such that for every $i \leq j$

$$e_i = e_j \circ f_{ij},$$

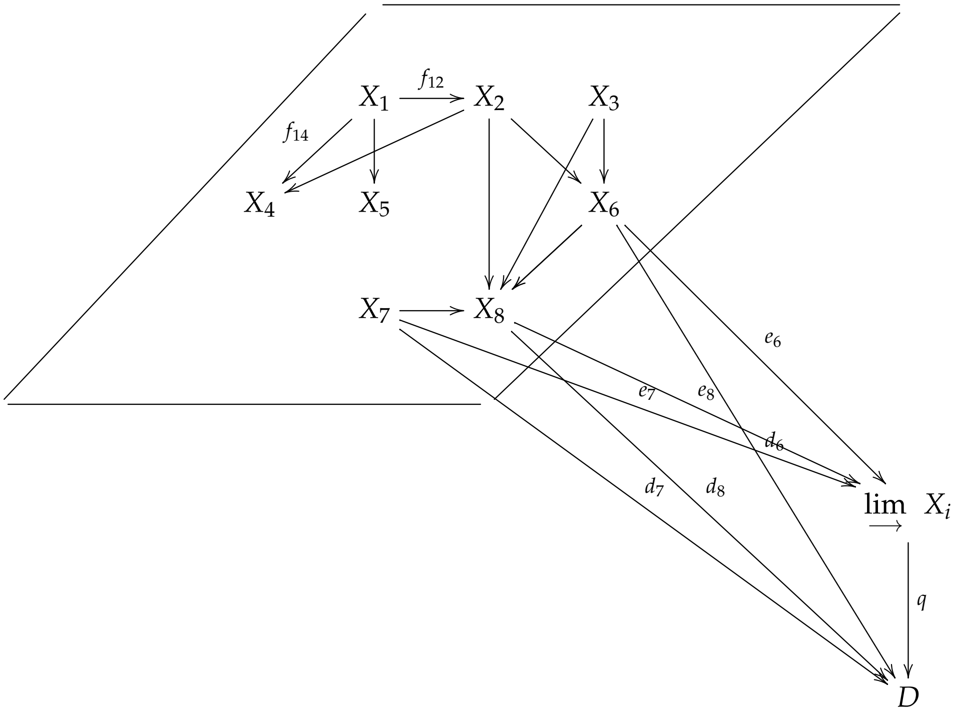
and having the following universal property: For any object D of **C** and collection of morphisms $d_i : X_i \to D$ that satisfy $d_i = d_j \circ f_{ij}$ for all $i \leq j$, there is a unique morphism

$$q : C \to D, \quad \text{such that } \ q \circ e_i = d_i, \forall i.$$

If such C exists, it is determined it up to a unique isomorphism by its universal property. We will denote it

$$\varinjlim \ X_i$$

(or $\varinjlim_{i\in I} \{X_i, f_{ij}\}$ if needed).



Proposition 13.1.1. *Direct limits exists in* **Sets**.

Proof. Let $S = \coprod_{i\in I}\{i\} \times X_i$. This is the precise way to talk about the disjoin union of the sets X_i. It is a set and we put on it an equivalence relation by saying that

$$(i, x) \sim (j, f_{ij}(x)), \quad \forall i \leq j \in I.$$

We call this situation an **elementary equivalence**. We force that to be a symmetric relation. This generates an equivalence relation. Two elements $(i, x), (j, y)$ are related if there is a finite sequence of elements related by elementary equivalences

$$(i, x) = (i_1, x_1) \sim (i_2, x_2) \sim \cdots \sim (i_n, x_n) = (j, y).$$

Let C be the set of equivalence classes. We denote an element of C by $[(i, x)]$. Let us show that C is a direct limit.

First, we have the morphisms e_i given by the compositions

$$X_i \to S \to C, \quad x \mapsto (i, x) \mapsto [(i, x)].$$

They satisfy $e_j \circ f_{ij} = e_i$.

Now, given a set D with morphisms $d_i \colon X_i \to D$ satisfying $d_j \circ f_{ij} = d_i$, we define

$$q \colon C \to D, \qquad q([(i, x)]) = d_i(x).$$

This is a well-defined function and to prove that we need only check elementary equivalence. In this case, if $(i, x) \sim (j, f_{ij}(x))$ then $q([(j, f_{ij}(x))]) = d_j(f_{ij}(x)) = d_i(x) = q([(i, x)])$. Moreover, the function q satisfies $q(e_i(x)) = q([(i, x)]) = d_i(x)$, as required. It is also clear that this property determines q. □

13.1.1. *Direct sum.* Let I be a set, considered as a partially order set where $x \leq x$ for all $x \in I$, but otherwise no two elements of I are comparable. Given a collection of objects $\{X_i : i \in I\}$ of a category **C** we can consider it as a direct system indexed by I. In this case, the direct limit, if it exists, is called the **direct sum**, or **coproduct**, and is denoted, respectively,

$$\oplus_{i\in I} X_i, \qquad \coprod_{i\in I} X_i.$$

Per definition, it comes with morphisms $e_i : X_i \to \coprod_{i\in I} X_i$ such that given any object D of **C** and morphisms $d_i \colon X_i \to D$, there is a unique morphism

$$q : \coprod_{i\in I} X_i \to D, \quad q \circ e_i = d_i.$$

For example, if **C** is the category of sets the coproduct is the disjoint union.

Proposition 13.1.2. *Direct sums exist in* $_{\mathbf{R}}$**Mod**.

Proof. In this case we assume all the X_i are R-modules. We define

$$\oplus_{i\in I} X_i$$

as the set of functions $f \colon I \to \coprod_{i\in I} X_i$, from I into the set theoretic disjoint union of the X_i, such that $f(i) \in \{i\} \times X_i$ and for all but finitely many i, $f(i) = (i, 0)$. We will be more colloquial and say that $f(i) \in X_i$. We will also just write

$$(a_i)_{i\in I} \in \oplus_{i\in I} X_i,$$

to denote the function $f(i) = a_i$ (or, to be precise, $f(i) = (i, a_i)$); in this notation

$$a_i \in X_i, \quad a_i = 0, \text{ for almost all } i.$$

We make this into an R-module by

$$(a_i)_i + (b_i)_i = (a_i + b_i)_i, \quad r(a_i)_i = (ra_i)_i.$$

We have natural module homomorphisms

$$X_i \to \oplus_{i\in I} X_i, \quad a \mapsto e_i(a),$$

where

$$(e_i(a))_j = \begin{cases} a, & j = i, \\ 0, & j \neq i. \end{cases}$$

Now, given an R-module M and homomorphisms $d_i \colon X_i \to M$, define

$$q \colon \oplus_{i\in I} X_i \to M, \qquad (a_i)_i \mapsto \sum_i d_i(a_i).$$

The sum is over a possibly infinite set, but only finitely many of the terms are non-zero and the meaning of the sum is that one sums only the non-zero terms. This map is a well-defined homomorphism of R-modules and satisfies $q \circ e_i = d_i$. It is also the unique possible homomorphism with this property: if q' has the same property then $q'((a_i)_i) = q'(\sum_i e_i(a_i)) = \sum_i q'(e_i(a_i)) = \sum_i d_i(a_i)$. □

Let us now strengthen this proposition and prove the following.

Theorem 13.1.3. *Arbitrary direct limits exist in* $_{\mathbf{R}}$**Mod**.

Proof. Let $\{X_i, f_{ij}\}$ be a direct system. Let $W \subseteq \oplus_i X_i$ be the R-submodule generated by all elements of the form $e_i(a_i) - e_j(f_{ij}(a_i))$, and let

$$C = (\oplus_i X_i)/W.$$

Thus, in C we have $e_i(a_i) = e_j(f_{ij}(a_i))$.

Denote by $\pi\colon \oplus_i X_i \to C$ the natural map and define

$$\tilde{e}_i\colon X_i \to C, \quad \tilde{e}_i := \pi \circ e_i.$$

We claim that C with the maps $\{\tilde{e}_i\}$ is the direct limit $\varinjlim \{X_i, f_{ij}\}$. First,

$$\tilde{e}_j(f_{ij}(a_i)) = \pi(e_j f_{ij}(a_i)) = \pi(e_i(a_i)) = \tilde{e}_i(a_i).$$

Next, given a module M and maps $d_i\colon X_i \to M$ such that $d_i \circ f_{ij} = d_j$, we find the following situation:

$$\begin{tikzcd}
X_i \arrow[r, "f_{ij}"] \arrow[drr, "e_i"] \arrow[ddrr, "\tilde{e}_i"] \arrow[dddr, "d_i"'] & X_j \arrow[dr, "e_j"] \arrow[ddr, "\tilde{e}_j"'] \arrow[ddd, "d_j"] & \\
 & & \oplus_i X_i \arrow[d, "\pi"] \arrow[ddl, "q"'] \\
 & & C \arrow[dl, "q'"] \\
 & M &
\end{tikzcd}$$

As $q(e_i(a_i) - e_j(f_{ij}(a_i))) = d_i(a_i) - d_j(f_{ij}(a_i)) = 0$, the map q factors through C and we get a homomorphism

$$q'\colon C \to M.$$

It satisfies

$$q' \circ \tilde{e}_i = q' \circ \pi \circ e_i = q \circ e_i = d_i.$$

This the unique homomorphism with this property: if $q'_1\colon C \to M$ has the same property, define $q_1\colon \oplus_i X_i \to M$ by $q_1 = q'_1 \circ \pi$. It satisfies $q_1 \circ e_i = q'_1 \circ \pi \circ e_i = q'_1 \circ \tilde{e}_i = d_i$. As $\oplus_i X_i$ is the direct limit of the system $\{X_i\}$, we have $q_1 = q$ and so $q'_1 = q'$. □

Not every category has direct limits. For example, let **C** be the category of finite sets and consider the direct system with the natural inclusion map

$$X_1 = \{1\} \overset{f_{12}}{\to} X_2 = \{1,2\} \overset{f_{23}}{\to} X_3 = \{1,2,3\} \overset{f_{34}}{\to} X_4 = \{1,2,3,4\} \overset{f_{45}}{\to} \dots$$

That is, for every $i \leq j$ the map

$$f_{ij}\colon X_i \to X_j,$$

is simply the inclusion map.

Suppose that a direct limit $\{C, e_i\}$ exists in the category **C**. Let $n \geq 1$ and $M = X_n$. Consider the maps $d_i\colon X_i \to M$ given by the natural inclusion $X_i \subset X_n$ for $i \leq n$ and for $i > n$ we have

$$d_i(x) = \begin{cases} x, & x \leq n, \\ n, & x > n. \end{cases}$$

We have for $i \leq j$ the compatibility $d_j \circ f_{i,j} = d_i$ and so there is a map $q\colon C \to M$ such that $q \circ e_i = d_i$. As the function d_n is injective, so must be the function e_n and that shows $|C| \geq n$ for all n. Thus, C is not a finite set and we get a contradiction.

The construction of direct limits in the category of rings is an involved business. However, one can prove easily that a direct system of rings over a *directed* index set does have a direct limit. See Exercise 38. This case is very important in geometry. Given a manifold X (in some category: algebraic varieties, complex manifolds, differential manifolds, topological spaces,...) and a point $x \in X$ we look at the system of all open sets V containing x. For every V we have the ring of functions $\mathcal{O}(V)$ on V; their description depends on the category. For real manifolds, for example, these will be the continuous maps $V \to \mathbb{R}$. For complex manifolds these will be the complex analytic maps $V \to \mathbb{C}$, and so on. The local ring $\mathcal{O}_{X,x}$ at the point x is the direct limit of rings $\varinjlim \mathcal{O}(V)$ under the natural restriction maps $\mathcal{O}(V) \to \mathcal{O}(U)$ if $U \subseteq V$. That is, the index set I which is directed, has elements that are the open sets V containing x and where $V \leq U$, if $U \subseteq V$.

13.1.2. *Pushout.* **Pushout** in a category **C** is a particular case of a direct limit, where the diagram is simply

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \\
C &
\end{tikzcd}$$

Thus, the pushout P, if it exists, will be an object P with morphisms as indicated in the following diagram, which is required moreover to commute:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "e_B"'] \\
C \arrow[r, "e_C"] & P
\end{tikzcd}$$

It has the universal property

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "e_B"'] \arrow[ddr, "d_B"] & \\
C \arrow[r, "e_C"] \arrow[drr, "d_C"'] & P \arrow[dr, "q"'] & \\
& & M
\end{tikzcd}$$

We know it exists in the category **Sets** and it is easy to see that it has the more concise description of

$$B \coprod C / \sim,$$

where $\sim$ is the equivalence relation generated by $\forall a \in A, f(a) \sim g(a)$.

We know the pushout exists in the category $_{\mathbf{R}}\mathbf{Mod}$, where it also affords the more compact description

$$B \oplus C/W,$$

where W is the submodule generated by $\{(f(a), -g(a)) : a \in A\}$.

13.1.3. *Amalgamated product.* Another very useful case is the pushout in the category of groups. We have a system of group homomorphisms

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \\
C &
\end{tikzcd}$$

And the pushout is called the **amalgamated product**, denoted $B *_A C$. It plays an important part in topology: Let Z be a connected and locally path-connected topological space and $Z = X \cup Y$ an open cover so that X, Y and $X \cap Y$ are likewise connected and locally path-connected. Let $t \in X \cap Y$ be a point.

Theorem 13.1.4 (Seifert-Van Kampen)**.**

$$\pi_1(X \cup Y, t) \cong \pi_1(X, t) *_{\pi_1(X \cap Y, t)} \pi_1(Y, t).$$

We define the group $B *_A C$ as the set of all finite length words

$$x_1 \cdots x_n,$$

where $x_i \in B \coprod C$ and subject to the equivalence relation generated by the following requirements:

(1) If for some i, x_i and x_{i+1} are in the same group then

$$x_1 \cdots x_n \sim x_1 \cdots x_{i-1}(x_i x_{i+1})x_{i+2} \cdots x_n.$$

(2) If for some i, $x_i = 1$ then

$$x_1 \cdots x_n \sim x_1 \cdots x_{i-1}x_{i+1} \cdots x_n.$$

(3) for every i and $a \in A$, if $x_i \in B$, we have

$$x_1 \cdots x_n \sim x_1 \cdots (x_i f(a))(g(a)^{-1}x_{i+1}) \cdots x_n,$$

(which implies $x_1 \cdots (x_i f(a))x_{i+1} \cdots x_n \sim x_1 \cdots x_i(g(a)x_{i+1}) \cdots x_n$) and if $x_i \in C$ we have

$$x_1 \cdots x_n \sim x_1 \cdots (x_i g(a))(f(a)^{-1}x_{i+1}) \cdots x_n.$$

It is easy to check that if we define multiplication by concatenation of words this gives a group structure on the equivalnece classes, providing us with the definition of the group $B *_A C$. If $A = \{1\}$ is the trivial group, it plays no role and we just use the notation $B * C$ and call it the **free product** of B and C.

An alternative way to define $B *_A C$ is as the group generated by the symbols $B \coprod C$ modulo the relations xyz^{-1} whenever x, y are in the same group and $z = xy$ and the further relations $f(a)g(a)^{-1}$ for all $a \in A$.

The construction seems very similar to the construction of the free group and there is a good reason for it. If $X = \{x_1, \dots, x_n\}$ and we let $G_i = \langle x_i \rangle$ the free cyclic group generated by x_i (isomorphic to $\mathbb{Z}$, but written multiplicatively) then

$$F(X) = G_1 * G_2 * \cdots * G_n,$$

the **free product** of the groups G_i. We should note that the terminology "amalgamated product" or "free product" is confusing because in the categorical sense these are more sums than products: for example $G_1 * G_2$ is the coproduct of G_1 and G_2 (and we often use the terminology direct sum for a coproduct) and not the product.

There are natural group homomorphisms

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "e_B"'] \\ C \arrow[r, "e_C"] & B *_A C \end{tikzcd}$$

Let M be a group and suppose that we have a diagram

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "e_B"'] \arrow[ddr, "d_B"] & \\
C \arrow[r, "e_C"] \arrow[drr, "d_C"'] & B *_A C \arrow[dr, "q"] & \\
 & & M
\end{tikzcd}$$

where we need to define the map q and show that it has the required properties. There is only one possibility:

$$q(x_1 \cdots x_n) = q(x_1) \cdots q(x_n), \qquad q(x_i) = \begin{cases} d_B(x_i), & x_i \in B, \\ d_C(x_i) & x_i \in C. \end{cases}$$

We leave the verification that this provides $B *_A C$ with the required universal property as an exercise.

The structure of the amalgamated product is in general very difficult to understand. For example, $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ is a much more complicated group than one may anticipate. The matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ has order 2 in $\mathrm{PSL}_2(\mathbb{Z})$ and the matrix $\left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ has order 3 (even in $\mathrm{SL}_2(\mathbb{Z})$). We have an induced homomorphism

$$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} \to \mathrm{PSL}_2(\mathbb{Z}).$$

One can prove that it is an isomorphism! Another example, is $\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z} *_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/6\mathbb{Z}$ using the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ that has order 4 in $\mathrm{SL}_2(\mathbb{Z})$ and the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ that has order 6 (Serre: *Trees*, §1.5.3).

Example 13.1.5. Let Z be the union of two circles touching at the point $t = (1, 0)$:

$$Z = \{(x, y) : (x^2 + y^2 - 1)((x-1)^2 + y^2 - 1) = 0\}.$$

We let $X = Z \cap \{(x, y) : x < 1.1\}, Y = Z \cap \{(x, y) : x > 0.9\}$. X and Y are homotopic to a circle and so, by standard results in topology, they have the same fundamental group as the circle, namely $\mathbb{Z}$. $X \cap Y$ is contractible to a point and so has trivial fundamental group. Thus, by the Seifert - van Kampen theorem,

$$\pi_1(Z, t) \cong \mathbb{Z} * \mathbb{Z} = F(x, y),$$

is the free group on the alphabet x, y.

13.2. **Inverse limits.**

The discussion concerning inverse limits is very similar, only that everything is "upside down". Let I be a poset and $\mathbf{C}$ a category, and consider a system $\{X_i, f_{ij}\}$ of objects of $\mathbf{C}$ and morphisms

$$f_{ij} : X_j \to X_i,$$

whenever $i \leq j$ such that $f_{ii} = 1_{X_i}$ and for $i \leq j \leq k$ we have $f_{ik} = f_{jk} \circ f_{jk}$. Such a system is called a **projective system**, or **inverse system**.

The **projective limit** (or **inverse limit**, or simply "limit") is "the object above the diagram that is closest to it". When it exists, it is characterized by its universal property – it's unique up to unique isomorphism and denoted

$$\varprojlim X_i.$$

Namely, it is an object C with morphisms $p_i \colon C \to X_i$ that satisfy $f_{ij} \circ p_j = p_i$ and that is universal relative to this property in the sense that given an object D with morphisms $q_i \colon D \to X_i$

satisfying $f_{ij} \circ q_j = q_i$ there is a unique morphism $r\colon D \to C$ satisfying $p_i \circ r = q_i$ for all i. In diagram,

$$\begin{tikzcd}
D \arrow[d, "r"] \arrow[ddr, "q_i"] \arrow[ddrr, "q_j"] \arrow[dd, dotted, bend right] & & \\
C \arrow[dr, "p_i"'] \arrow[drr, "p_j"] \arrow[d, dotted] & & \\
\cdots & X_i \arrow[l, dotted] & X_j \arrow[l, "f_{ij}"]
\end{tikzcd}$$

13.2.1. *Direct product.* As for direct limits, we start with the simplest example of index set I that is discrete. In this case, the projective limit is called a **direct product** (the use of verb "direct" is unfortunate, but is commonplace) and denoted

$$\prod_i X_i.$$

Proposition 13.2.1. *Products exist in the category* **Sets**.

Proof. The elements of $\prod_i X_i$ are functions $f\colon I \to \cup_i X_i$ with the property that $f(i) = x_i \in X_i$ for all i. We will usually denote such a function by $(x_i)_i$. Define the projection functions

$$p_i\colon \prod_i X_i \to X_i, \qquad p_i((x_j)_{j\in I}) = x_i.$$

Given D, define $r(d) = (q_i(d))_i$. Clearly $p_i \circ r = q_i$ and that r is the unique function with this property. □

Theorem 13.2.2. *Arbitrary projective limits exist in* **Sets**.

Proof. Consider the set C of vectors $(x_i)_i \in \prod_i X_i$ that satisfy $x_i = f_{ij}(x_j)$ for every $i \leq j$. Denote by

$$p_i\colon C \to X_i$$

the restriction of the maps p_i to C. We claim that $\{C, p_i\}$ is the projective limit. Firstly,

$$(f_{ij} \circ p_j)((x_\ell)_\ell) = f_{ij}(x_j) = x_i = p_i((x_\ell)_\ell).$$

Then, given D and morphisms q_i as in the definition, define

$$r\colon D \to C, \quad r(d) = (q_i(d))_i.$$

This element indeed lies in C because $f_{ij}(q_j(d)) = q_i(d)$. Clearly $p_i \circ r = q_i$ and we see that r is the unique function with this property. □

13.2.2. *General projective limits.* We prove two very useful results.

Theorem 13.2.3. *Arbitrary projective limits exist in* ${}_{\mathbf{R}}$**Mod** *and* **Rings**.

Proof. The construction and proofs are very similar to the case of **Sets**, so we'll be brief. In the category ${}_{\mathbf{R}}$**Mod**, for a projective system $\{M_i, f_{ij}\}$, define

$$\varprojlim M_i = \{(m_i)_i \in \prod_i M_i : f_{ij}(m_j) = m_i,\ i \leq j\}.$$

It is an R-module under coordinate-wise addition and $r(m_i)_i := (rm_i)_i$. The projections p_i simply take $(m_j)_j$ to m_i.

In the category **Rings** , for a projective system $\{R_i, f_{ij}\}$, define

$$\varprojlim R_i = \{(r_i)_i \in \prod_i R_i : f_{ij}(r_j) = r_i, i \leq j\}.$$

It is a ring under coordinate-wise addition and multiplication and it has an identity element that is the constant function 1. The projection p_i simply takes $(r_j)_j$ to r_i. □

A particular case of this construction is when I is a discrete set, in which case we get the direct product of modules and of rings. Note that if I is a finite set we have in the category of modules, $\prod M_i = \coprod M_i$, but for I infinite, these are different notions. Also note that the direct product of rings $\prod R_i$ always exists, while the direct sum of rings need not exist.

13.2.3. *Pullback.* This is a particular case of projective limits. Given a diagram

$$\begin{tikzcd} & A \arrow[d, "f"] \\ B \arrow[r, "g"] & C \end{tikzcd}$$

the **pullback**, if it exists, is the projective limit. In particular, it is an object X with morphism $X \to A, X \to B$ making the following diagram commutative:

$$\begin{tikzcd} X \arrow[r] \arrow[d] & A \arrow[d, "f"] \\ B \arrow[r, "g"] & C \end{tikzcd}$$

We know already that pullbacks exist in **Sets**, **Rings**, $_{\mathbf{R}}$**Mod**. In all these cases they afford the more compact description

$$\{(a, b) : a \in A, b \in B, f(a) = g(b)\}.$$

In a geometrical setting, the pullback is called **fibre product** and it "always" exists; it is a very important construction. For example, in Exercise 44, one proves that if A, B and C are topological spaces then the pushout, denoted in this case $A \times_C B$, is again the subset

$$\{(a, b) : a \in A, b \in B, f(a) = g(b)\}$$

of $A \times B$, with the induced topology.

13.3. **Completion of a ring.** Let R be a commutative ring and I an ideal of R. Then for every n, I^n is an ideal. Recall that it is the ideal generated over R by all length n products $x_1 \cdots x_n$ with all $x_j \in I$. Thus,

$$I \supseteq I^2 \supseteq I^3 \supseteq \dots.$$

There are natural ring homomorphisms that give us an inverse system over a directed index set

$$\dots \to R/I^3 \to R/I^2 \to R/I.$$

The projective limit, sometimes denoted $\hat{R}$, or $R^{\wedge I}$, is a ring with the following description:

$$\{(\dots, r_{n+1}, r_n, \dots, r_2, r_1) : r_n \in R/I^n, r_{n+1} \equiv r_n \pmod{I^n}\}.$$

It is called the **completion** of the ring R relative to the ideal I. Note that there is a natural map

$$R \to \hat{R}, \qquad r \mapsto (\dots, r, r, r).$$

Recall that a commutative ring is called **Noetherian** if any increasing sequence of ideals stabilizes. Namely, if $I_1 \subseteq I_2 \subseteq I_3$ is an increasing chain of ideals then for some n we have $I_n = I_{n+1} = I_{n+2} = \dots.$ Classical examples are the following: by a theorem of Hilbert, if R is a commutative Noetherian ring so is $R[x]$ and any quotient of it. As $\mathbb{Z}$ and any field k are Noetherian rings, we find, for example, that $k[x_1, x_2]/(x_1^3 - x_1 + 5x_2)$ is Noetherian and also that $\mathbb{Z}[i][x, y]$ is Noetherian. Indeed, $\mathbb{Z}[t]$ is Noetherian and so $\mathbb{Z}[i] \cong \mathbb{Z}[t]/(t^2 + 1)$ is Noetherian. Therefore, $\mathbb{Z}[i][x]$ is Noetherian and hence $(\mathbb{Z}[i][x])[y] = \mathbb{Z}[i][x, y]$ is Noetherian.

A commutative ring R is called a domain if it has no zero divisors. A fundamental theorem is the following.

Theorem 13.3.1 (Krull). *Let R be a noetherian domain and $I \neq R$ an ideal of R. The natural map*

$$R \to R^{\wedge I},$$

is injective.

In the following we discuss two interesting examples.

13.3.1. *Power series.* Let A be a commutative ring, $R = A[x_1, \dots, x_n]$ the ring of polynomials in n variables over A and let $I = (x_1, \dots, x_n)$. Then

$$R^{\wedge I} = A[\![x_1, \dots, x_n]\!],$$

is the ring of power series in n variables over A. If we use the notation $x^I = x_1^{i_1} \cdots x_n^{i_n}$ for $I = (i_1, \dots, i_n)$ a vector of non-negative integers, then

$$A[\![x_1, \dots, x_n]\!] = \left\{ \sum_I a_I x^I : a_I \in A \right\}.$$

(The summation is over all vectors I with non-negative integer components.) We leave the proof as an exercise. We have a natural inclusion $A[x_1, \dots, x_n] \subseteq A[\![x_1, \dots, x_n]\!]$. The completion of a ring is an algebraic way to arrive at analysis.

13.3.2. *p-adic numbers.* In this case we take our ring to be $\mathbb{Z}$ and our ideal to be $p\mathbb{Z}$, where p is a prime. The ring of **p-adic numbers** $\mathbb{Z}_p$ can be defined in the following way:

$$\mathbb{Z}_p = \mathbb{Z}^{\wedge p\mathbb{Z}} = \{(\dots, r_{n+1}, r_n, \dots, r_2, r_1) : r_n \in \mathbb{Z}/p^n\mathbb{Z}, r_{n+1} \equiv r_n \pmod{p^n}\}.$$

We can endow $\mathbb{Z}_p$ with additional structure. Give each $\mathbb{Z}/p^n\mathbb{Z}$ the discrete topology. Then $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ is a compact (by Tychonoff's theorem) Hausdorff topological space which is totally disconnected and so $\mathbb{Z}_p$, being a closed subset of $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$, is compact, Hausdorff and totally disconnected as well. Moreover, the ring operations (addition, multiplication, subtraction) are continuous. We can even make $\mathbb{Z}_p$ into a metric space (see Exercise 45).

Every element x of $\mathbb{Z}_p$ can be described as

$$x = \sum_{n=0}^{\infty} a_n(x) p^n,$$

where $a_i(x) \in \{0, 1, \dots, p-1\}$. Indeed, if an element of $\mathbb{Z}_p$ is $(r_n)_{n \geq 1}$, $\sum_{n=0}^{d} a_n p^n$ is just the expression of r_{d+1} as an element of $\mathbb{Z}/p^{d+1}\mathbb{Z}$ using usual base-p development. Given that, it is easy to see that the ideal $p^d\mathbb{Z}_p$ is the sums $\sum_{n=d}^{\infty} a_n p^n$, corresponding to the sequences $\{(\dots, r_{d+1}, 0, \dots, 0, 0)\}$. Projection on the d-th coordinate thus gives an isomorphism

$$\mathbb{Z}_p / p^d\mathbb{Z}_p \cong \mathbb{Z}/p^d\mathbb{Z}.$$

A sequence x_i converges in $\mathbb{Z}_p$ if and only if for every positive integer d there is an N such that for $i \geq N$ the d initial terms of the x_i agree. Namely, for $i \geq N$ and $j = 0, \dots, d$ we have

$$a_j(x_i) = a_j(x_N).$$

The description of elements as infinite sums is convenient. However, we should be careful about how operations are performed. For example, we have

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \dots$$

When we add 1 to $(p-1)+(p-1)p+(p-1)p^2+\dots$ we need to carry over:

$$\begin{aligned}1+(p-1)+(p-1)p+(p-1)p^2+\dots &= p+(p-1)p+(p-1)p^2+\dots\\ &= pp+(p-1)p^2+(p-1)p^3+\dots\\ &= pp^2+(p-1)p^3+\dots\\ &= \dots\\ &= 0.\end{aligned}$$

If $p=5$ then

$$\begin{aligned}(2+2\cdot 5+2\cdot 5^2+\dots)\times(3+3\cdot 5+3\cdot 5^2+\dots) &= 6+12\cdot 5+18\cdot 5^2+24\cdot 5^3\dots\\ &= 1+3\cdot 5^2+3\cdot 5^4+\dots\end{aligned}$$

(the pattern does not continue). Incidentally, note that $(1+1\cdot 5+1\cdot 5^2+\dots)=\frac{1}{1-5}=\frac{1}{4}$.

Consider the closely related limit over $n\geq 1$

$$\varprojlim\ \mathbb{Z}/p^n\mathbb{Z}[x],$$

which is the completion of the ring of polynomials $\mathbb{Z}[x]$ relative to the ideal $p\mathbb{Z}[x]$.

This limit is denoted $\mathbb{Z}_p\langle x\rangle$ and is an example of a **Tate algebra**; those play an important role in the development of analysis over the p-adic numbers.

Proposition 13.3.2. *The ring $\mathbb{Z}_p\langle x\rangle$ admits the following concrete description:*

$$\mathbb{Z}_p\langle x\rangle=\{\sum_{n=0}^{\infty}a_nx^n : a_n\in\mathbb{Z}_p, a_n\to 0\}.$$

Proof. Suppose given a sum like that. Then, for every N there is n such that $a_i\in p^N$ for $i>n$. Define the polynomials

$$P_N(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}/p^N\mathbb{Z}[x].$$

Note that

$$P_N(x)\equiv P_{N+1}(x)\pmod{p^N}.$$

Thus, the vector $(\dots,P_3(x),P_2(x),P_1(x))$ is a well-defined element of $\mathbb{Z}_p\langle x\rangle$. The map

$$\{\sum_{n=0}^{\infty}a_nx^n : a_n\in\mathbb{Z}_p, a_n\to 0\}\to\mathbb{Z}_p\langle x\rangle$$

is a ring homomorphism ($P_N(x)$ is essentially $\sum_{n=0}^{\infty}a_nx^n \pmod{p^N}$) and it is injective, because $P_N=0$ for all N implies $a_i\equiv 0\pmod{p^N}$ for all i and N and this implies $a_i=0$ for all i.

To show it's surjective, we assume given a sequence of polynomials $P_N(x)\in\mathbb{Z}/p^N\mathbb{Z}[x]$ such that $P_N(x)=\sum_{i=0}^{\infty}a_i(N)x^i$ where only finitely many coefficients are non-zero and

$$P_N(x)\equiv P_{N+1}(x)\pmod{p^N}.$$

But that means that for every i, $a_i(N)\equiv a_i(N+1)\pmod{p^N}$. Therefore, the sequence $(a_i(N))_{N=1}^{\infty}$ is a p-adic number α_i such that $\alpha_i\equiv a_i(N)\pmod{p^N}$ for all N. It follows that $\sum_{n=0}^{\infty}\alpha_nx^n$ is a preimage of the sequence $(\dots,P_3(x),P_2(x),P_1(x))$. □

14. Infinite Galois groups

14.1. **Review of finite Galois theory.** The content of this section should be well-familiar from MATH 457. Let $\mathbb{F}$ be a field. A polynomial $f(x) \in \mathbb{F}[x]$ is called separable if it has distinct roots; equivalently, $\gcd(f(x), f'(x)) = 1$. A field $\mathbb{F}$ is perfect if it either has characteristic 0, or it has characteristic p and the map $x \to x^p$ is surjective. This includes all finite fields. An irreducible polynomial over a perfect field is separable.

Let $f(x) \in \mathbb{F}[x]$. A splitting field for f is a field $L \supseteq \mathbb{F}$ in which the polynomial $f(x)$ factors, $f(x) = a\prod_{i=1}^{n}(x - \alpha_i)$, $a, \alpha_i \in L$, and $L = \mathbb{F}(\alpha_1, \dots, \alpha_n)$. A basic result is that any two splitting fields for f are isomorphic over $\mathbb{F}$. In fact, if $\sigma : \mathbb{F} \to \tilde{\mathbb{F}}$ is an isomorphism of fields taking $f(x)$ to $\tilde{f}(x)$, and if L (resp. $\tilde{L}$) is a splitting field for f (resp., for $\tilde{f}$) then there's a commutative diagram

$$\begin{tikzcd}
L \arrow[r, "\tilde{\sigma}", "\cong"'] & \tilde{L} \\
\mathbb{F} \arrow[u, hook] \arrow[r, "\sigma", "\cong"'] & \tilde{\mathbb{F}} \arrow[u, hook]
\end{tikzcd}$$

The key is the following: if f is irreducible, $\alpha \in L$ is a root, then $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/(f(x)) \cong \tilde{\mathbb{F}}[x]/(\tilde{f}(x)) \cong \tilde{\mathbb{F}}(\tilde{\alpha})$ for a root $\tilde{\alpha}$ of $\tilde{f}$ in $\tilde{L}$. The proof of the general statement is done inductively and is useful in calculating Galois groups.

A field extension $K/\mathbb{F}$ is called algebraic if every element of K solves some non-zero polynomial $f(x) \in \mathbb{F}[x]$. Every finite extension is algebraic. An algebraic extension $K/\mathbb{F}$ is called separable if every element of K is a root of a separable polynomial $f(x) \in \mathbb{F}[x]$. An extension $K/\mathbb{F}$ is called a normal extension if it's the splitting field for a collection of polynomials $\{f(x)\} \subset \mathbb{F}[x]$, meaning that they all split in K and K is generated over $\mathbb{F}$ by their roots. It is a theorem that if $K/\mathbb{F}$ is normal, $f(x) \in \mathbb{F}[x]$ is irreducible and has a root in K then $f(x)$ splits in K.

Automorphisms. Let $K/\mathbb{F}$ be a field extension. Define

$$\mathrm{Aut}(K/\mathbb{F}) = \{\sigma\colon K \to K \text{ a field automorhism}, \sigma|_F = id.\}.$$

Assume until further notice that $K/\mathbb{F}$ is a finite extension. We have the fundamental theorem:

Theorem 14.1.1. $|\mathrm{Aut}(K/\mathbb{F})| \leq [K : \mathbb{F}]$ *with equality if and only if K is the splitting field of a separable polynomial (equivalently, a collection of separable polynomials).*

We call an extension for which an equality holds a Galois extension and use $\mathrm{Gal}(K/\mathbb{F})$ for $\mathrm{Aut}(K/\mathbb{F})$ in this case.

Theorem 14.1.2. *Let $K/\mathbb{F}$ be a finite extension of fields. The following are equivalent:*

(1) $K/\mathbb{F}$ is Galois, i.e., $|\mathrm{Aut}(K/\mathbb{F})| = [K : \mathbb{F}]$.
(2) $\mathbb{F} = K^{\mathrm{Aut}(K/\mathbb{F})} := \{k \in K : \sigma(k) = k, \forall \sigma \in \mathrm{Aut}(K/\mathbb{F})\}$.
(3) K is the splitting field of a separable polynomial $f(x) \in \mathbb{F}[x]$.
(4) $K/\mathbb{F}$ is a normal and separable extension.

A key example is the following theorem: Let $K/\mathbb{F}$ be any extension of fields, not necessary finite, and $G \subseteq \mathrm{Aut}(K/\mathbb{F})$ a finite group. Then K/K^G is a Galois extension with Galois group G.

In general, we have two maps for an extension $K/\mathbb{F}$:

$$\text{subgroup } G \subseteq \mathrm{Aut}(K/\mathbb{F}) \quad \mapsto \quad K^G = \{k \in K : \sigma(k) = k, \forall \sigma \in G\}$$

$$K \supseteq L \supseteq F \quad \mapsto \quad G_L = \{\sigma \in \mathrm{Aut}(K/\mathbb{F}) : \sigma|_L = id.\}$$

We have

$$G_{K^G} \supseteq G, \quad K^{G_L} \supseteq L.$$

For $K/\mathbb{F}$ a finite Galois extension these are inverses correspondences:

Theorem 14.1.3 (Main Theorem of Galois theory)**.** *Let $K/\mathbb{F}$ be a finite Galois extension, $G = \mathrm{Gal}(K/\mathbb{F})$. There's a bijection*

$$\{\textit{subfields } K \supseteq L \supseteq F\} \longleftrightarrow \{\textit{subgroups } H \subseteq G\}.$$

Under this bijection $L \mapsto G_L = \mathrm{Aut}(K/L)$, $H \mapsto K^H$. The following holds:

(1) $H_1 \subseteq H_2 \Rightarrow K^{H_1} \supseteq K^{H_2}$.
(2) $K_1 \supseteq K_2 \Rightarrow \mathrm{Aut}(K/K_1) \subseteq \mathrm{Aut}(K/K_2)$.
(3) $K^{H_1} \cap K^{H_2} = K^{\langle H_1, H_2 \rangle}$, $K^{H_1}K^{H_2} = K^{H_1 \cap H_2}$.
(4) $[K : K^H] = |H|, \quad [K^H : \mathbb{F}] = [G : H]$.
(5) For every subgroup H, K/K^H is Galois with Galois group H.
(6) For a subgroup H, $K^H/\mathbb{F}$ is Galois if and only if H is normal in G. In this case, $\mathrm{Gal}(K^H/\mathbb{F}) = G/H$.

14.2. **Infinite Galois extensions.** Let $K/\mathbb{F}$ be an algebraic extension of fields, possibly of infinite degree. We that that $K/\mathbb{F}$ is **Galois** if it also separable and normal. That is, every $k \in K$ solves a separable non-zero polynomial $f(x) \in \mathbb{F}[x]$ and any irreducible polynomial $f(x) \in \mathbb{F}[x]$ that has a root in K splits into linear factors over K.

Lemma 14.2.1. *Let $K/\mathbb{F}$ be an algebraic extension. Then $K/\mathbb{F}$ is Galois if and only if $K = \cup_L L$, is a union of finite Galois extensions $L/\mathbb{F}$ contained in K.*

Proof. Exercise! □

Suppose that $K/\mathbb{F}$ is Galois. The set $\{L : L \text{ is a finite Galois extension of } \mathbb{F}, \text{ contained in } K\}$ is a direct poset I under inclusion. Given L_1, L_2 Galois , L_1L_2 is Galois over $\mathbb{F}$ and $L_i \subseteq L_1L_2$. If $L_1 \subseteq L_2$ we have a surjection $\mathrm{Gal}(L_2/\mathbb{F}) \to \mathrm{Gal}(L_1/\mathbb{F})$. Thus, $\{\mathrm{Gal}(L/\mathbb{F}) : L \in I\}$ is an inverse system. Let

$$G = \varprojlim \mathrm{Gal}(L/\mathbb{F}) \quad (\text{limit over all } L/F \text{ finite Galois inside } K).$$

Lemma 14.2.2. $G = \mathrm{Aut}(K/\mathbb{F})$.

Proof. Exercise! □

Let us give each finite group $\mathrm{Gal}(L/\mathbb{F})$ the discrete topology. Then $\mathrm{Aut}(K/\mathbb{F})$, that we also denote $\mathrm{Gal}(K/\mathbb{F})$, has a natural topology, being a closed subgroup of the compact topological group $\prod_{L\in I} \mathrm{Gal}(L/\mathbb{F})$. In this topology it is compact, Hausdorff and totally disconnected.

14.3. **Profinite groups.** More generally, let G be a **profinite group**. That is

$$G = \varprojlim_{\alpha \in I} G_\alpha,$$

where G_α are finite groups, I a directed poset and for $\alpha \leq \beta$ the homomorphisms $f_{\alpha\beta} \colon G_\beta \to G_\alpha$ are *surjective*.

Each G_α is given the discrete topology. As

$$G = \{(g_\alpha)_\alpha : g_\alpha \in G_\alpha, f_{\alpha\beta}(g_\beta) = g_\alpha, \forall \alpha \leq \beta\} \subseteq \prod_{\alpha \in I} G_\alpha$$

is a closed subgroup of a compact (Tychonoff's theorem), Hausdorff topological group, it is itself a compact Hausdorff topological group (meaning, the group operation and the inverse are continuous maps).

Lemma 14.3.1. *(1) Every open subgroup of G is closed and has finite index in G. It contains a subgroup of the form*

$$G_J := G \cap \left(\prod_{\alpha \notin J} G_\alpha \times \prod_{\alpha \in J} \{1\} \right),$$

for some finite subset $J \subseteq I$. G_J is open. Every open set $U \subseteq G$ is a union of cosets of G_J's.

(2) Every closed subgroup of finite index of G is open.

(3) The intersection of open subgroups is a closed subgroup. Every closed subgroup is the intersection of open subgroups.

Proof. Exercise! (two observations are useful: for $g \in G$ multiplication by g is an automorphism of G and so H is open implies xH is open. The other is that by the definition of the topology every open set containing the identity contains some G_J. For (2) show that $H = \cap_J HG_J$, and note that as the G_J are normal the HG_J are subgroups.) □

14.4. **The Galois group of an arbitrary Galois extension.** Taking into account the topology of the Galois group of a possibly infinite Galois extension we can extend the fundamental theorem.

Theorem 14.4.1 (Main Theorem of infinite Galois theory)**.** *Let $K/\mathbb{F}$ be a Galois extension, $G = \mathrm{Gal}(K/\mathbb{F})$. There is bijection*

$$\{K \supseteq M \supseteq \mathbb{F}\} \quad \leftrightarrow \quad \{\textit{closed subgroups } H \subseteq G\}$$

under which $M \mapsto H_M = \{\sigma \in G : \sigma|_M = id.\}$ and $H \mapsto K^H = \{k \in K : \sigma(k) = k, \forall \sigma \in G\}$. These maps are mutual inverses. Furthermore:

(1) M is a finite extension of $\mathbb{F}$ if and only if H_M is open.

(2) K/M is a Galois extension with Galois group H_M.

(3) $M/\mathbb{F}$ is Galois if and only if $H_M \lhd G$ and in this case $\mathrm{Gal}(M/\mathbb{F}) \cong G/H_M$.

Proof. This is not very hard, but is harder than the previous claims I left as exercises. If I have time I will type the proof. □

Part 5. **Commutative algebra**

15. Localization of rings and modules

Let R be a commutative ring. The process of localization of R is a way to force certain subsets of R to become invertible by suitably enlarging the ring.

15.1. **Localizing a ring.**

Let R be a *commutative* ring and let $S \subseteq R$ be a subset. S is called **multiplicative** if $1 \in S$ and $x, y \in S \Rightarrow xy \in S$.

Example 15.1.1. Here are some of the most important examples:

(1) $S = \{1, f, f^2, \dots\}$ for some element $f \in R$.
(2) If $\mathfrak{p} \lhd R$ is a prime ideal then $S = R - \mathfrak{p}$ is a multiplicative set.
(3) If R is an integral domain then $S = R - \{0\}$ is a multiplicative set (note that this is a special case of the previous example).

Let S be a multiplicative set. The construction of the ring $R[S^{-1}]$ mimics the construction of the rational numbers from the integers. Consider first the set of *formal* fractions

$$\left\{ \frac{r}{s} : r \in R, s \in S \right\}.$$

Define a relation on it by saying that

$$\frac{r}{s} \sim \frac{r'}{s'} \Leftrightarrow \exists s'' \in S,\ s''(s'r - sr') = 0.$$

We leave as an exercise to check that this is an equivalence relation.

To make the notation simpler we will use $\frac{r}{s}$ also to denote the equivalence class of a formal fraction $\frac{r}{s}$. The collection of these classes is denoted $R[S^{-1}]$ and is called the **localization of** R **at** S. But, of course, any definition we make will have to be checked to be independent of choice of representatives. We define two operations on $R[S^{-1}]$:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_2 r_1 + s_1 r_2}{s_1 s_2}, \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

We leave it as an exercise to check that these are well-defined and turn $R[S^{-1}]$ into a commutative ring (whose zero element 0 is the equivalence class of $\frac{0}{1}$ and whose identity element 1 is the equivalence class of $\frac{1}{1}$). There is a ring homomorphism,

$$\ell \colon R \to R[S^{-1}], \qquad r \mapsto \frac{r}{1}.$$

If $s \in S$ then $\ell(s)$ is invertible. Indeed, $\ell(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1} = 1$. In fact, the homomorphism $\ell \colon R \to R[S^{-1}]$ has the universal property for maps $f \colon R \to B$ into commutative rings B such that $f(s)$ is invertible in B for all $s \in S$. Every such map factors uniquely:

$$\begin{tikzcd} R \arrow[r, "\ell"] \arrow[dr, "f"'] & R[S^{-1}] \arrow[d] \\ & B \end{tikzcd}$$

The ring homomorphism ℓ is not necessarily injective.

Lemma 15.1.2. $\mathrm{Ker}(\ell) = \{r \in R : \exists s \in S, sr = 0\}$.

Example 15.1.3. Let R be an integral domain; for example, $\mathbb{Z}$ or $\mathbb{C}[x]$. Let $S = R - \{0\}$. Then the ring $R[S^{-1}]$ is a field and in fact is the minimal field containing R. It is called the **field of fractions** of R. Some common notations are $\mathrm{Frac}(R)$ or $\mathrm{Quot}(R)$. For example, for $\mathbb{Z}$ we obtain the field of rational numbers $\mathbb{Q}$, and for $\mathbb{C}[x]$ we obtain the **field of rational functions** $\mathbb{C}(x) = \left\{\frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{C}[x], g(x) \neq 0\right\}$.

15.2. **Localizing a module.** Let M be an R-module. There are two approaches to defining the **localization** $M[S^{-1}]$ **of** M at a multiplicative set S of R. The first is to define

$$M[S^{-1}] := R[S^{-1}] \otimes_R M.$$

Using everything we know about tensor products, we see that localization becomes a functor:

$$_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{R}[\mathbf{S}^{-1}]}\mathbf{Mod}.$$

We will return to this point of view in the next section.

The other approach, which is very useful for calculations, is to mimic the construction of $R[S^{-1}]$. Namely, we begin by considering the set of formal fractions

$$\left\{\frac{m}{s} : m \in M, s \in S\right\}.$$

Define a relation on it by saying that

$$\frac{m}{s} \sim \frac{m'}{s'} \Leftrightarrow \exists s'' \in S,\ s''(s'm - sm') = 0.$$

Note that in particular $\frac{m}{s} = 0$ if and only if there is an $s' \in S$ such that $s'm = 0$.

Let us check that this is an equivalence relation. It is clear that this relation is reflexive and symmetric. Suppose now that $\frac{m_1}{s_1} \sim \frac{m_2}{s_2}$ and $\frac{m_2}{s_2} \sim \frac{m_3}{s_3}$. Then, for some $t_1, t_2 \in S$ we have $t_1(s_2m_1 - s_1m_2) = t_2(s_3m_2 - s_2m_3) = 0$. From this we get that $t_1t_2s_3(s_2m_1 - s_1m_2) = 0$ and $t_1t_2s_1(s_3m_2 - s_2m_3) = 0$. Adding those two expressions, we find that $t_1t_2s_3s_2m_1 - t_1t_2s_1s_2m_3 = 0$, or that $t_1t_2s_2(s_3m_1 - s_1m_3) = 0$. Since $t_1t_2s_2 \in S$ that means that $\frac{m_1}{s_1} \sim \frac{m_3}{s_3}$. Note that even if initially $t_1 = t_2 = 1$ we don't end with the conclusion that $s_3m_1 - s_1m_3 = 0$ but only with $s_2(s_3m_1 - s_1m_3) = 0$. This explains why the equivalence relation was defined that way.

As before, to keep the notation simpler we will use $\frac{m}{s}$ also to denote the equivalence class of a formal fraction $\frac{m}{s}$. We define an $R[S^{-1}]$-module structure on $M[S^{-1}]$:

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2m_1 + s_1m_2}{s_1s_2}, \qquad \frac{r}{s_1} \cdot \frac{m}{s_2} = \frac{r \cdot m}{s_1s_2}.$$

One checks that these are well defined and turn $M[S^{-1}]$ into an $R[S^{-1}]$-module. There is a map

$$\ell \colon M \to M[S^{-1}], \qquad m \mapsto \frac{m}{1},$$

which is a group homomorphism with the property

$$\ell(rm) = \ell(r)\ell(m).$$

These two descriptions of $M[S^{-1}]$ are really the same. There is a map

$$R[S^{-1}] \otimes_R M \to M[S^{-1}], \quad \frac{r}{s} \otimes m \mapsto \frac{r \cdot m}{s}.$$

The inverse is $\frac{m}{s} \mapsto \frac{1}{s} \otimes m$. To prove that, it is useful to note that every element of $R[S^{-1}] \otimes_R M$ can be written as $\frac{1}{s} \otimes m$ by using a common denominator and the relation $\frac{r}{s} \otimes m = \frac{1}{s} \otimes (rm)$.

If $\mathfrak{p}$ is a prime ideal and $S = R - \mathfrak{p}$, we will denote $M_{\mathfrak{p}}$ the localization $M[S^{-1}]$. If $S = \{1, f, f^2, \dots\}$ we will denote $R[S^{-1}]$ by $R[f^{-1}]$.

15.3. **Localization is an exact functor.** Let **C** be an additive full subcategory of a category ${}_{\mathbf{R}}\mathbf{Mod}$ such that the zero module 0 belongs to **C** and **C** is closed under taking kernels and quotients.[8] A sequence of modules and module morphisms

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

is called a **short exact sequence** if the image of every map is the kernel of the following one. Namely: (i) f is injective; (ii) g is surjective; (iii) $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

Suppose that **D** is another category with the properties **C** has. A covariant additive functor $F\colon \mathbf{C} \to \mathbf{D}$ with the property[9] $F(0) = 0$ is called **exact** if for any short exact sequence

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

in **C**, the sequence

$$\begin{tikzcd} 0 \arrow[r] & FA \arrow[r, "Ff"] & FB \arrow[r, "Fg"] & FC \arrow[r] & 0 \end{tikzcd}$$

in **D** is a short exact sequence as well. In general this need not be the case: for example, the functors $M \otimes_R (-)$, $\mathrm{Hom}_R(M, -)$ are typically not exact, but only "1/2 exact". The study of this failure is the origin of homological algebra and understanding the modules for which the functors are exact is an important part, leading to concepts such as projective, injective and flat modules.

Lemma 15.3.1. *Localizaton is an exact functor.*

Proof. Let R be a commutative ring, S a multiplicative set and $\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$ an exact sequence of R-modules. We need to prove that

$$\begin{tikzcd} 0 \arrow[r] & A[S^{-1}] \arrow[r, "f"] & B[S^{-1}] \arrow[r, "g"] & C[S^{-1}] \arrow[r] & 0 \end{tikzcd}$$

is an exact sequence of $R[S^{-1}]$-modules.

If $f(\frac{a}{s}) = 0$ then $\frac{f(a)}{s} = 0$ and that means that for some $s' \in S$ we have $s'f(a) = 0$. But, $s'f(a) = f(s'a)$ and since f is injective, $s'a = 0$. But that means that $\frac{a}{s} = 0$.

We have $g(f(\frac{m}{s})) = \frac{g(f(m))}{s} = \frac{0}{s} = 0$. And, given $c \in C$ there is a $b \in B$ such that $g(b) = c$. Thus, $g(\frac{b}{s}) = \frac{c}{s}$ and we get that g is surjective.

It remains to show that $\mathrm{Ker}(g) \subset \mathrm{Im}(f)$. Suppose that $g(\frac{b}{s}) = \frac{g(b)}{s} = 0$. Then, there is $s' \in S$ such that $0 = s'g(b) = g(s'b) = 0$. Thus, there is $a \in A$ such that $f(a) = s'b$. We now find that $f(\frac{a}{s's}) = \frac{s'b}{s's} = \frac{b}{s}$. □

15.4. **Prime ideals and localization.**

Proposition 15.4.1. *Let R be a commutative ring and $S \subset R$ a multiplicative set. There is a bijection between the prime ideals of $R[S^{-1}]$ and the prime ideals of R that do not intersect S.*

Proof. Let I be an ideal of $R[S^{-1}]$ then $I^c := \ell^{-1}(I)$ (the "c" stands for "contracted") is an ideal of R. Furthermore, we have an inclusion

$$R/I^c \hookrightarrow R[S^{-1}]/I.$$

[8] We are avoiding here introducing the highly technical definition of an **abelian category**. By the Freyd-Mitchell theorem, every abelian category is equivalent, by means of an additive functor, to a full-subcategory of the category of modules ${}_{\mathbf{R}}\mathbf{Mod}$ for some (not necessarily commutative) ring R.

[9] In fact, $F(0) = 0$ automatically holds

If I is prime then $R[S^{-1}]/I$ is an integral domain, hence so is R/I^c. Therefore, I^c is a prime ideal of R. If $\exists s \in S \cap I^c$ then $\frac{s}{1} \in I$ and thus I contains a unit. It follows that $I = R[S^{-1}]$. But, by definition, a prime ideal is a proper ideal. Contradiction. Thus, I^c is a prime ideal of R that does not intersect S.

Conversely, given an ideal I of R, we have $I \subseteq R$ an inclusion of R modules, giving us an inclusion of $R[S^{-1}]$ modules $I[S^{-1}] \subseteq R[S^{-1}]$. That is, $I^e := I[S^{-1}]$ is an $R[S^{-1}]$ ideal (the "e" is for "extended").

Suppose that I is a prime ideal that doesn't intersect S. We want to show that I^e is prime. Suppose that $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in I^e$. Then, for some $a_3 \in I, s_3 \in S$ we have $\frac{a_1 a_2}{s_1 s_2} = \frac{a_3}{s_3}$ and thus, for some $s_4 \in S$ we have $s_4 s_3 a_1 a_2 = s_4 s_1 s_2 a_3 \in I$. As $s_4, s_3 \in S$, I is prime and $I \cap S = \emptyset$, we must have $a_1 a_2 \in I$ and, again, either $a_1 \in I$ or $a_2 \in I$. Therefore, either $\frac{a_1}{s_1} \in I^e$ or $\frac{a_2}{s_2} \in I^e$.

It remains to check that $I^{ce} = I$ for I a prime ideal of $R[S^{-1}]$, and $I^{ec} = I$ for I a prime ideal of R disjoint with S. The latter will also prove that $I^e \neq R[S^{-1}]$ and so, combined with the above, that I^e is a prime ideal.

Begin with the first case. Let $a \in I^c$. Then $\ell(a) = \frac{a}{1} \in I$ and so for any $s \in S$, $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} \in I$. That is, $I^{ce} \subseteq I$. Let $\frac{a}{s} \in I$. Then also $\frac{a}{1} = \frac{s}{1} \cdot \frac{a}{s} \in I$ and thus $a \in I^c$. But then $\frac{a}{s} \in I^{ce}$ and we get $I^{ce} \supseteq I$.

Now let I be a prime ideal of R disjoint with S. Let $a \in I$ then $\frac{a}{1} \in I^e$ and so $a \in I^{ec}$. Conversely, if $a \in I^{ec}$ then $\frac{a}{1} \in I^e$ and so for some $b \in I, s \in S$ we have $\frac{a}{1} = \frac{b}{s}$. Then, for some $s_1 \in S$ we have $s_1 s a = s_1 b$. As $s_1 b \in I$, I is prime and $s_1, s \notin I$, we conclude that $a \in I$. □

If the set $S = R - \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal, then one denotes the localization $R[S^{-1}]$ also by $R_\mathfrak{p}$ and refer to as the **localization by a prime ideal**. One calls a ring R a **local ring** if it has a unique maximal ideal. The Proposition implies that $R_\mathfrak{p}$ is a local ring whose unique maximal ideal is $\mathfrak{p}^e$. In fact, the prime ideals of $R_\mathfrak{p}$ correspond bijectively to prime ideals of R that are contained in $\mathfrak{p}$. Put differently, if we are interested only in the prime ideals of R that are contained in a given prime ideal $\mathfrak{p}$, we may pass to $R_\mathfrak{p}$ where the picture of ideals is simplified. The only prime ideals remaining come from those that are contained in $\mathfrak{p}$. This explains the terminology "localization".

16. The spectum of a ring

Let R be a commutative ring. Grothendieck associated to R a special kind of topological space denoted $\mathrm{Spec}(R)$. It has much more structure than merely a topology. It is a so-called locally ringed space. This definition was the basis for a revolution in algebraic geometry. In a blink of an eye algebraic geometry was extended from varieties that were associated to very special rings of the form $k[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle$ for some polynomials $f_1, \dots, f_n$ with coefficients in a field k, to a vast universe where any commutative ring is allowed. Besides a mere generalization this allowed the resolution of important foundational issues in algebraic geometry; for a long time the development of algebraic geometry was spearheaded by the "great Italian geometers", but a crisis in its foundations was brewing. Grothendieck's work allowed to re-write classical algebraic geometry and put it on solid foundations. From a different perspective it allowed a new kind of geometry that was essential to the development of arithmetic geometry. (See, for example, *Intuition and Rigor and Enriques's Quest* by David Mumford, Notices AMS 2011 and *How Grothendieck Simplified Algebraic Geometry* by Colin McLarty, Notices AMS 2016.) Grothendieck perhaps fully realized the beautiful saying of Sophie Germain (1776-1831): *"L'algèbre n'est qu'une géeométrie écrite; la géométrie n'est qu'une algèbre figurée"*.

16.1. Spec(R) **as a set.** Let R be a commutative ring. We define the set

$$\mathrm{Spec}(R) = \{[\mathfrak{p}] : \mathfrak{p} \text{ a prime ideal of } R\}.$$

Namely, the points in Spec(R) are the prime ideals of R. We use the brackets so as to distinguish between the point $[\mathfrak{p}]$ in the set Spec(R) and the actual prime ideal $\mathfrak{p}$.

Example 16.1.1. Here are a few simple examples:

(1) If R is a field, $\mathrm{Spec}(R) = \{[0]\}$. It is a singleton corresponding to the ideal $\{0\}$ of R.
(2) Likewise, if R is a field and t is a variable $\mathrm{Spec}(R[t]/(t^2))$ is a singleton corresponding to the unique prime ideal of this ring, the ideal (t). One often writes this ring as $R[\epsilon]$ where it is understood that $\epsilon^2 = 0$. It is called the **ring of dual numbers**.
(3) $\mathrm{Spec}(\mathbb{Z}) = \{[0], [2\mathbb{Z}], [3\mathbb{Z}], [5\mathbb{Z}], \dots\}$.
(4) $\mathrm{Spec}(\mathbb{C}[x]) = \{[0]\} \cup \{[(x-\alpha)] : \alpha \in \mathbb{C}\}$. Let us explain that:
Suppose that I is a prime ideal that is not 0. Then I contains some polynomial $f(x)$ that is not constant. As I is prime, it contains also the prime factors of f and so we may assume that f is irreducible. But such f must be a degree 1 polynomial. So $I \supseteq (x-\alpha)$ for some α. As the ideal $(x-\alpha)$ is maximal (the quotient $\mathbb{C}[x]/(x-\alpha) \cong \mathbb{C}$), it follows that $I = (x-\alpha)$.
(5) $\mathrm{Spec}(\mathbb{R}[x])$ is a bit more complicated. Besides points of the form $[(x-\alpha)], \alpha \in \mathbb{R}$ and $[0]$, it also contains points of the form $[(x^2+bx+c)]$ with $b^2 - 4c < 0$. These are all the points of $\mathrm{Spec}(\mathbb{R}[x])$.

The following lemma is clear.

Lemma 16.1.2. *A homomorphism of rings $f\colon R \to S$ induces a function*

$$f^*\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R), \qquad [\mathfrak{p}] \mapsto [f^{-1}(\mathfrak{p})].$$

Example 16.1.3. (1) The homomorphism $\mathbb{Z} \to \mathbb{F}_p$, embeds the point $\mathrm{Spec}(\mathbb{F}_p)$ as the point $[p\mathbb{Z}] \in \mathrm{Spec}(\mathbb{Z})$.
(2) The homomorphism $\mathbb{R}[x] \to \mathbb{C}[x]$ induces a function $\mathrm{Spec}(\mathbb{C}[x]) \to \mathrm{Spec}(\mathbb{R}[x])$ that takes the point $[(x-\alpha)]$ to the point $[(x-\alpha)]$ if $\alpha \in \mathbb{R}$ and to the point $[(x-\alpha)(x-\bar{\alpha})]$ if $\alpha \notin \mathbb{R}$.
(3) Let $h \in R$ and $S = \{1, h, h^2, \dots\}$ a multiplicative set. We will denote the localization $R[S^{-1}]$ by $R[h^{-1}]$. It is in fact isomorphic to $R[x]/(xh-1)$. By Proposition 15.4.1, the ring homomorphism
$$\ell\colon R \to R[h^{-1}]$$
gives an injective map $\mathrm{Spec}(R[h^{-1}]) \to \mathrm{Spec}(R)$ whose image is the set of prime ideals of R that do not contain h.

16.2. Spec(R) **as a topological space.** Before defining the topology, we consider the notion of a radical of an ideal. Let $\mathfrak{a} \lhd R$ be an ideal. Its **radical** $\sqrt{\mathfrak{a}}$ is

$$\sqrt{\mathfrak{a}} = \{r \in R : \exists n \geq 1, r^n \in \mathfrak{a}\}.$$

It is indeed an ideal. If $r \in \sqrt{a}$ and $r^n \in \mathfrak{a}$ then for every $s \in R$ also $(sr)^n = s^n r^n \in \mathfrak{a}$ and so $R\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a}}$. If $r_i \in \sqrt{\mathfrak{a}}$ and say $r_i^{n_i} \in \mathfrak{a}$ then $(r_1 + r_n)^{n_1+n_2}$ is, by the binomial formula, a sum of terms each of which is either a multiple of $r_1^{n_1}$ or of $r_2^{n_2}$, thus in $\mathfrak{a}$. Thus, $\sqrt{a}$ is an ideal containing $\mathfrak{a}$. The ideal $\mathfrak{a}$ is called a **radical ideal** if $\mathfrak{a} = \sqrt{\mathfrak{a}}$. For example, if $\mathfrak{a}$ is a prime ideal then it is a radical ideal. Also, for every ideal $\mathfrak{a}$, $\sqrt{\mathfrak{a}}$ is a radical ideal.

Now let $\mathfrak{a}$ be an ideal of R. Define a subset of Spec(R):

$$V(\mathfrak{a}) = \{[\mathfrak{p}] \in \mathrm{Spec}(R) : \mathfrak{p} \supseteq \mathfrak{a}\}.$$

We define a topology on $\mathrm{Spec}(R)$ whose closed sets are the $V(\mathfrak{a})$. Note that $V(\{0\}) = \mathrm{Spec}(R)$ and $V(R) = \emptyset$. To show this is a topology, we must prove the (1) & (3) of following lemma.

Proposition 16.2.1. *The following holds:*

(1) $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$.

(2) $V(\mathfrak{a}) = V(\mathfrak{b}) \Leftrightarrow \sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$.

(3) $\cap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$*, where* $\sum_i \mathfrak{a}_i$ *is the minimal ideal of* R *containing all the ideals* $\mathfrak{a}_i$.

Proof. We begin with the first claim. Any ideal containing $\mathfrak{a}$ (resp. $\mathfrak{b}$) contains $\mathfrak{a}\mathfrak{b}$, so the r.h.s contains the l.h.s. Let $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ be a prime ideal and suppose that $\mathfrak{p}$ doesn't contain $\mathfrak{b}$. There is thus $b \in \mathfrak{b}$ such that $b \notin \mathfrak{p}$. For every $a \in \mathfrak{a}$ the element $ab \in \mathfrak{a}\mathfrak{b}$ and so in $\mathfrak{p}$. As $\mathfrak{p}$ is prime and $b \notin \mathfrak{p}$ it must be that $a \in \mathfrak{p}$. It follows that $[\mathfrak{p}] \in V(\mathfrak{a})$.

For the second claim, we first note that if $\mathfrak{p} \supseteq \mathfrak{a}$ is a prime ideal then $\mathfrak{p} \supseteq \sqrt{a}$. Thus, $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$. So, it is enough to prove that the set of prime ideals $\mathfrak{p}$ that contain a given radical ideal determines it. In fact, we have the following lemma.

Lemma 16.2.2. *Let* $\mathfrak{a}$ *be an ideal of* R *then*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p},$$

the intersection being over prime ideals containing $\mathfrak{a}$.

Proof. One inclusion is clear. If $w^n \in \mathfrak{a}$ and $\mathfrak{p} \supseteq \mathfrak{a}$ is a prime ideal then $w^n \in \mathfrak{p}$ and so $w \in \mathfrak{p}$. That gives $\sqrt{\mathfrak{a}} \subseteq \cap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p}$.

Now, take an element $f \in R$ such that $f \notin \sqrt{a}$. That is, for all $n > 0$, $f^n \notin \mathfrak{a}$. Let Σ be the set of ideals $\mathfrak{b} \supseteq \mathfrak{a}$ of R with the property that $f^n \notin \mathfrak{b}$ for all $n > 0$. This is a non-empty set as $\mathfrak{a} \in \Sigma$; it is partially ordered under inclusion and every chain of ideals $\{\mathfrak{b}_\alpha\}_{\alpha \in I}$ has an upper bound $\cup_{\alpha \in I} \mathfrak{b}_\alpha$ that belongs to Σ. By Zorn's Lemma, Σ has a maximal element $\mathfrak{p}$. We claim that $\mathfrak{p}$ is a prime ideal and being in Σ, $\mathfrak{p} \supseteq \mathfrak{a}$ and $f \notin \mathfrak{p}$. Thus, we are done.

Suppose that $\mathfrak{p}$ is not a prime ideal. Then, there are $x, y \in R$ such that

$$xy \in \mathfrak{p}, \quad x \notin \mathfrak{p}, y \notin \mathfrak{p}.$$

Therefore, we have a strict inclusion of ideals $(x) + \mathfrak{p} \supsetneqq \mathfrak{p}$, $(y) + \mathfrak{p} \supsetneqq \mathfrak{p}$. Thus, for some n, m positive integers we have $f^n \in (x) + \mathfrak{p}, f^m \in (y) + \mathfrak{p}$, But then, $f^{m+n} \in ((x) + \mathfrak{p})((y) + \mathfrak{p}) \subseteq \mathfrak{p}$. Contradiction. □

The last claim is rather easy. If $\mathfrak{p}$ contains each $\mathfrak{a}_i$ it contains the minimal ideal containing all of them, and vice-versa. □

Note an interesting corollary of the lemma.

Corollary 16.2.3. *The* **nilradical** *of* R*, that is, the ideal* $\sqrt{0}$*, is the collection of all nilpotent elements of* R *and is equal to the intersection of all prime ideals of* R*:*

$$\sqrt{0} = \cap_{\mathfrak{p}\ prime} \mathfrak{p} = \{r \in R : \exists n > 0, r^n = 0\}.$$

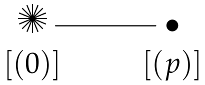
Returning to our main topic, we have established the existence of a topology on $\mathrm{Spec}(R)$ whose closed sets are the sets $V(\mathfrak{a})$.

Example 16.2.4. It is not hard to show that if $\mathfrak{p}$ is a prime ideal then $V([\mathfrak{p}])$ is the closure of the one point set $\{[\mathfrak{p}]\}$. Let's consider a few simple examples:

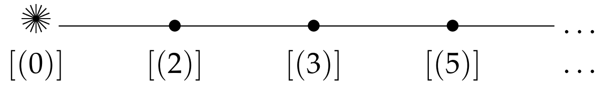
- If k is a field then $\mathrm{Spec}(k), \mathrm{Spec}(k[\epsilon]), \mathrm{Spec}(k[x, y, z]/(x^2, y^3, z^{11})$ are just one point spaces.

$$\overset{\bullet}{[(0)]}$$

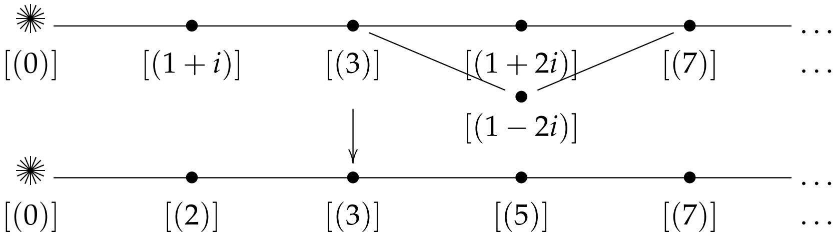
- Let p be a prime and consider $\mathrm{Spec}(\mathbb{Z}_{(p)})$. The prime ideals of $\mathbb{Z}_{(p)}$ correspond to the ideals of $\mathbb{Z}$ contained in (p) and there two of them (p) and (0). Thus,
$$\mathrm{Spec}(\mathbb{Z}_{(p)}) = \{[0], [(p)]\}.$$
The point $[(p)]$ is closed. The point $[0]$ is an open set whose closure is the whole of $\mathrm{Spec}(\mathbb{Z}_{(p)})$.



- Consider now $\mathrm{Spec}(\mathbb{Z})$. We know its points are $\{[0], [(2)], [(3)], [(5)], \dots\}$. Every point $[(p)]$ for p a prime number, is a closed point. The point $[(0)]$ is not an open set; it's closure is the whole of $\mathrm{Spec}(\mathbb{Z})$. Every non-empty open set contains all but finitely many closed points (in particular, it contains $[0]$), and conversely.



- The situations for rings of the form $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[e^{2\pi i/7}]$, and so on is similar, but the precise enumeration of the prime ideals becomes a number theoretic question. For example, for $\mathbb{Z}[i]$ we have closed points of the form (p) for every $p \equiv 3 \pmod 4$ and points of the form $[(x+yi)]$ and $(x-yi)$ for every prime $p \equiv 1 \pmod 4$, where x, y satisfy $x^2+y^2=p$. An additional closed point is $(1+i)$. There are all the closed points. The only additional point of $\mathrm{Spec}(\mathbb{Z}[i])$ is $[(0)]$ and it's dense.



Proposition 16.2.5. *Let $f\colon R \to S$ be a homomorphism of rings. Then the induced map*
$$f^*\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R)$$
is continuous.

Proof. We only need to calculate $(f^*)^{-1}(V(\mathfrak{a}))$ for an ideal $\mathfrak{a}$ of R. We claim that
$$(f^*)^{-1}(V(\mathfrak{a})) = V(\langle f(\mathfrak{a})\rangle).$$
(Here $\langle f(\mathfrak{a})\rangle$ is the ideal of S generated by the set $f(\mathfrak{a})$.) Indeed, if $\mathfrak{p}$ is an ideal of S that contains $f(\mathfrak{a})$ then $f^{-1}(\mathfrak{p}) \supseteq \mathfrak{a}$ and so $f^*[\mathfrak{p}] \in V(\mathfrak{a})$. That is, $\mathfrak{p} \in (f^*)^{-1}(V(\mathfrak{a}))$.

Conversely, if $\mathfrak{p} \in (f^*)^{-1}(V(\mathfrak{a}))$ then $f^*[\mathfrak{p}] = [f^{-1}(\mathfrak{p})] \in V(\mathfrak{a})$ so $f^{-1}(\mathfrak{p}) \supseteq \mathfrak{a}$ and it follows that $\mathfrak{p} \supseteq f(\mathfrak{a})$ and so $\mathfrak{p} \in V(\langle f(\mathfrak{a})\rangle)$. □

We have defined a topology by specifying the closed sets. There is a particular kind of open sets that is very convenient to work with. Let $f \in R$ and define
$$D(f) = \{[\mathfrak{p}] : f \notin \mathfrak{p}\} = \mathrm{Spec}(R) - V((f)).$$
If we think about elements of R as functions on $\mathrm{Spec}(R)$ (and we shall soon see that this is precisely the case) then we can think about $f \pmod{\mathfrak{p}}$ as the *value* of f at the point $[\mathfrak{p}]$. Denote

this value[10] $\bar{f}([\mathfrak{p}])$ then

$$\bar{f}([\mathfrak{p}]) = 0 \Leftrightarrow f \in \mathfrak{p}.$$

For example, if $R = \mathbb{C}[x_1, \dots, x_n]$ and $f(x_1, \dots, x_n)$ is in R, then at the closed point $[\mathfrak{p}] = [(x_1 - \alpha_1, \dots, x_n - \alpha_n)]$ defined by an n-tuple of complex numbers $\alpha_1, \dots, \alpha_n$, the value of f is classically $f(\alpha_1, \dots, \alpha_n)$, which is precisely $f \pmod{\mathfrak{p}}$. Under this interpretation of elements of R as functions, $D(f)$ is precisely the set where $f \neq 0$.

The sets $D(f)$ are a basis for the topology, i.e. they are open and any open set is a union of the sets $D(f)$. Indeed, if $[\mathfrak{p}] \notin V(\mathfrak{a})$ then there is an element $f \in \mathfrak{a}$ such that $f \notin \mathfrak{p}$. Then we see that $D(f)$ is an open set that is disjoint from $V(\mathfrak{a})$ and contains $[\mathfrak{p}]$.

Proposition 16.2.6. *The function* $\ell^* : \mathrm{Spec}(R[f^{-1}]) \to \mathrm{Spec}(R)$ *is a homemorphism onto* $D(f)$.

Proof. We have seen in Example 16.1.3 that this map is a bijection from $\mathrm{Spec}(R[f^{-1}])$ to $D(f)$, and Proposition 16.2.5 gives that this function ℓ^* is continuous. It remains to show that it is a closed map when $D(f)$ is provides with the induced topology.

Let $\mathfrak{a}$ be an ideal of $R[f^{-1}]$. We claim that $I \supseteq \mathfrak{a} \Leftrightarrow I^c \supseteq \mathfrak{a}^c$. One direction is obvious. Suppose that $I^c \supseteq \mathfrak{a}^c$ then $I = I^{ce} \supseteq \mathfrak{a}^{ce}$. So it only remains to check that $\mathfrak{a}^{ce} \supseteq \mathfrak{a}$, and, indeed if $\frac{a}{s} \in \mathfrak{a}$ then $\frac{a}{1} \in \mathfrak{a}$ and also $\frac{a}{1} \in \mathfrak{a}^{ce}$. But then also $\frac{a}{s} \in \mathfrak{a}^{ce}$.

Let $\mathfrak{a}$ be an ideal of $R[f^{-1}]$ then $\ell^*(V(\mathfrak{a}))$ is the set

$$\{I^c : I \supseteq \mathfrak{a}, I \text{ prime}\} = \{J \lhd R \text{ prime}, f \notin J, J \supseteq \mathfrak{a}^c\} = D(f) \cap V(\mathfrak{a}^c),$$

a closed set of $D(f)$. □

Let R be a ring and $n \geq 0$ an integer. One denotes

$$\mathbb{A}^n_R = \mathrm{Spec}(R[x_1, \dots, x_n]),$$

and calls it the n-dimensional **affine space over** R. Let us look more closely at two examples:

(1) **The complex affine line $\mathbb{A}^1_{\mathbb{C}} = \mathrm{Spec}(\mathbb{C}[x])$.** We have seen that the points of this space are $[0]$ and $[(x - \alpha)]$ for $\alpha \in \mathbb{C}$. The point $[0]$ is dense – its closure is the whole space. Every other point $[\mathfrak{p}]$ is a closed point, namely, the closure of the set $\{[\mathfrak{p}]\}$ is itself.

Every non-zero ideal $\mathfrak{a}$ is of the form $(f(x))$ and the set $V(\mathfrak{a})$ consists of the points $[(x - \alpha)]$ such that $(x - \alpha) | f(x)$, namely, of the points $[(x - \alpha)]$ such that $f(\alpha) = 0$. So, closed sets correspond to zeros of polynomials. One can also check that the complement of $V((f))$ is $D(f)$ – the points where f doesn't vanish.

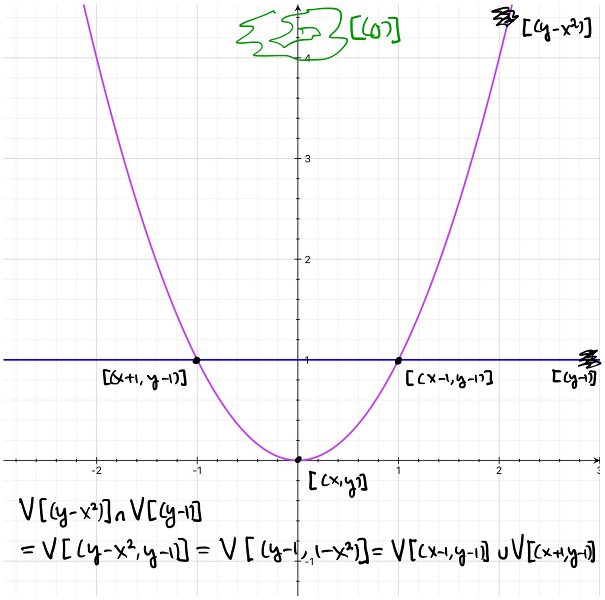
(2) **The complex affine plane $\mathbb{A}^2_{\mathbb{C}} = \mathrm{Spec}(\mathbb{C}[x, y])$.** The description requires two difficult results that are a special case of Hilbert's Nullstellensatz and Krull's Hauptidealsatz. They say, in this case, that

(a) every maximal ideal of $\mathbb{C}[x, y]$ is of the form $(x - \alpha, y - \beta)$, and

(b) besides (0) every other prime ideal of $\mathbb{C}[x, y]$ is of the form $(f(x, y))$ where $f(x, y) \in \mathbb{C}[x, y]$ is an irreducible polynomial, determined uniquely up to multiplication by a scalar.

The closure of the point $[(0)]$ is the whole $\mathbb{A}^2_{\mathbb{C}}$. If $f(x, y)$ is irreducible, the closure of a point $[(f(x, y))]$ is the point itself together with all the points $[(x - \alpha, y - \beta)]$ such that $f(\alpha, \beta) = 0$. The points $[(x - \alpha, y - \beta)]$ are closed. It requires additional commutative algebra to conclude that every closed set of $\mathbb{A}^2_{\mathbb{C}}$ is a finite union of these basic closed sets. For a polynomial $f(x, y) \neq 0$, the set $D(f)$ is the open set containing all points $[(x - \alpha, y - \beta)]$ such that $f(\alpha, \beta) \neq 0$ and all points $[(g(x, y))]$ such that g is irreducible and $g \nmid f$. Namely, its complement is the union of the sets $V([(g(x, y))])$ where $g(x, y)$ varies over all irreducible factors of $f(x, y)$.

[10] We use $\bar{f}([\mathfrak{p}])$ and not just $f([\mathfrak{p}])$ because soon we will use the notation $f([\mathfrak{p}])$ to denote something differnt.



16.3. Spec(R) **as a locally ringed space.** The additional structure one puts on Spec(R) is that of a sheaf. We therefore begin by introducing this notion.

16.3.1. *Sheaves.* Let X be a topological space. A **sheaf** $\mathcal{O}$ of abelian groups (resp., commutative rings) on X is the following data:

(1) (*values*) For each open set U an abelian group (resp. commutative ring) $\mathcal{O}(U)$, with $\mathcal{O}(\emptyset) = 0$.
(2) (*restriction maps*) For each inclusion $V \subseteq U$ a homomorphism $res_{UV}\colon \mathcal{O}(U) \to \mathcal{O}(V)$ of groups (resp., rings) such that (i) $res_{UU} = Id$ and (ii) for $V \subseteq U \subseteq W$ we have $res_{UV} \circ res_{WU} = res_{WV}$.
(3) (*locally zero is zero*) If $U = \cup U_i$ and $s \in \mathcal{O}(U)$ is such that $res_{UU_i}(s) = 0$ for all i, then $s = 0$.
(4) (*local data can be glued*) If $U = \cup U_i$ and $s_i \in \mathcal{O}(U_i)$ are elements such that for all i, j, $res_{U_i, U_i \cap U_j}(s_i) = res_{U_j, U_i \cap U_j}(s_j)$ then there exists $s \in \mathcal{O}(U)$ such that $res_{UU_i}(s) = s_i$ for all i.

A **ringed space** X is a topological space with a sheaf of rings $\mathcal{O}_X$. Given then a point $x \in X$ we can form the ring of **germs of functions** (also called **stalk**) at x by

$$\mathcal{O}_{X,x} = \varinjlim_{x \in U} \mathcal{O}_X(U),$$

the limit taken over all open sets U containing x. As the index set here is directed, we can think about an element of this ring as a pair

$$(U, f)$$

consisting of an open set U containing x and $f \in \mathcal{O}_X(U)$, and where two pairs $(U, f), (V, g)$ are considered the same element in $\mathcal{O}_{X,x}$ if $res_{U,U\cap V}(f) = res_{V,U\cap V}(g)$. We will also write the last equation more transparently as $f|_{U\cap V} = g|_{U\cap V}$. In this language, for example,

$$(U_1, f_1) + (U_2, f_2) = (U_1 \cap U_2, f_1|_{U_1\cap U_2} + f_2|_{U_1\cap U_2}).$$

In general, the ring $\mathcal{O}_{X,x}$ need not be a local ring; a local ring R, by definition, is a ring that has a unique maximal ideal. This need not be the case for $\mathcal{O}_{X,x}$. A ringed space $(X, \mathcal{O}_X)$ is called a **locally ringed space** if the sheaf of rings $\mathcal{O}_X$ has the property that all the rings $\mathcal{O}_{X,x}$ are local rings. We then refer to $\mathcal{O}_{X,x}$ as the **local ring of** x.

Example 16.3.1. Let $U \subset \mathbb{R}^n$ be an open set. Then, defining for an open set $V \subseteq U$,

$$\mathcal{O}(V) = \{f \colon V \to \mathbb{R}, \text{ continuous}\},$$

makes U into a locally ringed space. The maximal ideal of the ring $\mathcal{O}_x$ are all the pairs (V, f) such that $f(x) = 0$. Similarly, if we choose to define

$$\mathcal{O}(V) = \{f : V \to \mathbb{R}, f \text{ is } C^\infty\},$$

we would get a different locally ringed space (with the same underlying topological space).

Example 16.3.2. A Riemann surface with its sheaf of analytic functions is a locally ringed space.

Example 16.3.3. Let a be a symbol and consider $\{a\}$ is a topological space with one point. Define a sheaf on it by $\mathcal{O}(\{a\}) = R$, where R is some ring. Then $\mathcal{O}_a = R$. If R is not a local ring this is a ringed space that is not a locally ringed space.

16.3.2. *The sheaf on* Spec(R). We wish to make $X = \text{Spec}(R)$ into a locally ringed space. We first note that following: for $[\mathfrak{p}] \in \text{Spec}(R)$ the ring $R_\mathfrak{p}$ is a local ring; its unique maximal ideal is the localization of $\mathfrak{p}$. Thus, we wish to define a sheaf of rings $\mathcal{O}$ on Spec(R) with the property that $\mathcal{O}_{[\mathfrak{p}]} = R_\mathfrak{p}$. We do that as follows:

For an open set U let $\mathcal{O}(U)$ be functions f on U with the property that for all $[\mathfrak{p}] \in U$ we have $f(\mathfrak{p}) \in R_\mathfrak{p}$ and such that f is locally a ratio of two elements of R. Namely, for each $[\mathfrak{p}] \in U$ exists an open set $V \subseteq U$ containing $[\mathfrak{p}]$ and elements r, s of R such that $s \notin \mathfrak{q}$ for all points $[\mathfrak{q}] \in V$ and such that $f = \frac{r}{s}$ in $R_\mathfrak{q}$ for all $[\mathfrak{q}] \in V$.

Given two functions f, g, in $\mathcal{O}(U)$ we define $f + g$ by $(f + g)([\mathfrak{p}]) = f([\mathfrak{p}]) + g([\mathfrak{p}])$, and similarly for products. One needs to check that the sum and product, thus defined, are also "locally fractions" and that is easy. This gives $\mathcal{O}(U)$ a ring structure. The natural restriction maps for $V \subseteq U$ are indeed ring homomorhisms $\mathcal{O}(U) \to \mathcal{O}(V)$. Given an open cover $U = \cup_i U_i$, and $f \in \mathcal{O}(U)$ such that $f|_{U_i} = 0$, clearly $f = 0$. Given functions $f_i \in \mathcal{O}(U_i)$ such that $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ we define a function f on U by $f([\mathfrak{q}]) = f_i([\mathfrak{q}])$ if $[\mathfrak{q}] \in U_i$. This is well-defined. The only further verification required is that f is locally a fraction. It is enough to show that $f|_{U_i}$ is locally a fraction, but that is clear because $f|_{U_i} = f_i$.

We therefore get a sheaf of rings on Spec(R) making it into a ringed space. To show it is a locally ringed space we prove the following lemma.

Lemma 16.3.4. *There is a natural isomorphism* $\mathcal{O}_{[\mathfrak{p}]} \cong R_\mathfrak{p}$.

Proof. Any element of $\mathcal{O}_{[\mathfrak{p}]}$ has a representative (U, f), where U is an open set containing $\mathfrak{p}$, and we associate it the value $f([\mathfrak{p}]) \in R_\mathfrak{p}$. This is independent of the representative and provides a ring homomorphism $\mathcal{O}_{[\mathfrak{p}]} \to R_\mathfrak{p}$.

Suppose that (U, f) is mapped to zero. There is an open set V containing $[\mathfrak{p}]$ such that on V the function f is a fraction $\frac{r}{s}$. By definition, there is some $s_1 \in R - \mathfrak{p}$ such that $s_1 r = 0$. The open set $D(s_1) \cap V$ contains $[\mathfrak{p}]$ and on it f is zero: for each point $[\mathfrak{q}]$ in it, $f = \frac{r}{s}$ is also zero in $R_\mathfrak{q}$ because $s_1 r = 0$ and $s_1 \notin \mathfrak{q}$. So we have $(U, f) = (D(s_1) \cap V, f|_{D(s_1) \cap V}) = (D(s_1) \cap V, 0) = 0$.

Finally, our map is surjective. Let $\frac{r}{s} \in R_\mathfrak{p}$, then $(D(s), \frac{r}{s})$ is a well-defined element of $\mathcal{O}_{[\mathfrak{p}]}$ mapping to $\frac{r}{s}$ under our ring homomorphism. □

Remark 16.3.5. One can show that

$$\mathcal{O}(D(f)) = R[f^{-1}],$$

the localization of R in the multiplicative set $\{1, f, f^2, \dots\}$ (See *Hartshorne, Algebraic Geometry*, Springer, Graduate Text in Mathematics). That requires some effort and we will not prove this result here. However, we will use it, and the next Proposition, it in the sequel. Note that, in particular, taking $f = 1$ we find

$$\mathcal{O}(\mathrm{Spec}(R)) = R.$$

Remark 16.3.6. Let $(X, \mathcal{O}_X)$ be a locally ringed space and $U \subseteq X$ an open subset. The **induced sheaf** $\mathcal{O}_X|_U$ is defined as follows: for $V \subseteq U$ open let

$$V \mapsto \mathcal{O}_X(V).$$

It is immediate that this is a sheaf of rings making $(U, \mathcal{O}_X|_U)$ into a locally ringed space (with the same local rings!)

Proposition 16.3.7. *Let $f \in \mathrm{Spec}(R)$, then $D(f)$ with the induced sheaf $\mathcal{O}_X|_{D(f)}$ is isomorphic to* $\mathrm{Spec}(R[f^{-1}])$.

16.3.3. *Functoriality.* It is natural to expect at this point that a ring homomorphism $f\colon R \to S$ would produce a morphism of locally ringed spaces

$$f^*\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R).$$

This is correct, but we haven't yet defined what it means.

To begin with we define a morphism of sheaves: Let X be a topological space and $\mathscr{F}, \mathscr{G}$, two sheaves of commutative rings on X. A **morphism of sheaves**

$$h\colon \mathscr{F} \to \mathscr{G}$$

is a collection of ring homomorphisms

$$h_U\colon \mathscr{F}(U) \to \mathscr{G}(U),$$

such that for all $V \subseteq U$ the following diagram commutes:

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r, "h_U"] \arrow[d, "res_{UV}"] & \mathscr{G}(U) \arrow[d, "res_{UV}"] \\
\mathscr{F}(V) \arrow[r, "h_V"] & \mathscr{G}(V)
\end{tikzcd}$$

If we think of $\mathscr{F}, \mathscr{G}$, as functors from the poset of open sets of X to commutative rings, h is just a natural transformation of functors.

Let $(X, \mathcal{O}_X), (Y, \mathcal{O}_Y)$, be ringed spaces. Suppose that $f\colon X \to Y$ is a continuous map. Then, we get a new sheaf of rings on Y, denoted $f_*\mathcal{O}_X$ defined by

$$f_*\mathcal{O}_X(U) = \mathcal{O}_X(f^{-1}(U)).$$

We leave the verification that this is a sheaf of rings as an exercise. A priori there is no relation between $\mathcal{O}_Y(U)$ and $\mathcal{O}_X(f^{-1}(U))$ as the sheaves are not guaranteed to be sheaves of functions on X or Y (although in almost any application they are...). Thus, we also specify a homomorphism of sheaves

$$f^\sharp : \mathcal{O}_Y \to f_*\mathcal{O}_X.$$

Heuristically, $f^\sharp$ tells us how to pull back "functions" from Y to X. Indeed, in many situations the map $f^\sharp$ is so obvious that it doesn't require mentioning at all. A **morphism of ringed spaces** is thus such a pair:

$$(f, f^\sharp)\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y),$$

where $f\colon X \to Y$ is a continuous map and $f^\sharp\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$ is a morphism of sheaves.

For example, suppose that X, Y, are topological spaces and $\mathcal{O}_X, \mathcal{O}_Y$, are the sheaves of real-valued continuous functions on X, Y, respectively. Then we can let $f^\sharp$ be composition with f.

For every open set $U \subset Y$ and $g\colon U \to \mathbb{R}$ a continuous map, let $f^\sharp(g) := g \circ f$; it is a continuous function on $f^{-1}(U)$. That is, $f^\sharp(g) \in f_*\mathcal{O}_X(U)$.

Returning to the general case, let $x \in X$ and $y = f(x)$. We claim that we have a natural map

$$\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}.$$

Let I be the poset of open sets of Y that contain y and J the open sets of X that contain x. Then

$$\mathcal{O}_{Y,y} = \varinjlim_{U \in I} \mathcal{O}_Y(U), \quad \mathcal{O}_{X,x} = \varinjlim_{U \in J} \mathcal{O}_X(U).$$

The homomorphisms $f^\sharp$ then provide maps

$$\mathcal{O}_{Y,y} = \varinjlim_{U \in I} \mathcal{O}_Y(U) \xrightarrow{f^\sharp} \varinjlim_{U \in I} \mathcal{O}_X(f^{-1}(U)) \longrightarrow \varinjlim_{V \in J} \mathcal{O}_X(V) = \mathcal{O}_{X,x}.$$

(This is perhaps easiest to check if we think about elements of the local rings as equivalence classes of pair (U, g).)

Suppose that $(X, \mathcal{O}_X), (Y, \mathcal{O}_Y)$, are locally ringed spaces and

$$(f, f^\sharp) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

is a morphism of ringed spaces. To be a **morphism of locally ringed spaces** we make the additional requirement that for all $x \in X$ the induced ring homomorphism

$$f^\sharp : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$$

is a **local homomorphism**. Namely, that $f^{\sharp,-1}(\mathfrak{m}_x) = \mathfrak{m}_{f(x)}$, where $\mathfrak{m}_x$ (resp. $\mathfrak{m}_{f(x)}$) is the maximal ideal of $\mathcal{O}_{X,x}$ (resp. $\mathcal{O}_{Y,f(x)}$).

16.4. **An equivalence of categories.** By definition, an affine scheme is a locally ringed space isomorphic as a locally ringed space to $(\mathrm{Spec}(R), \mathcal{O})$ for some ring R. Morphisms of affine schemes are morphisms of locally ringed spaces. Thus, affine schemes are a full subcategory **Aff**.**Sch** of the category of locally ringed spaces.

Theorem 16.4.1. *The category of affine schemes is anti-equivalent to the category* **Com**.**Rings** *of commutative rings.*

Proof. We define a functor

$$\textbf{Com}.\textbf{Rings} \to \textbf{Aff}.\textbf{Sch}$$

by sending a ring R to $\mathrm{Spec}(R)$. Let $f\colon R \to S$ be a homomorphism of rings. We associate to it a morphism

$$(f^*, f^\sharp)\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R).$$

We have already defined f^* as $f^*([\mathfrak{p}]) = [f^{-1}(\mathfrak{p})]$, and showed it is a continuous map of topological spaces. To ease notation, write

$$X = \mathrm{Spec}(S), \quad Y = \mathrm{Spec}(R).$$

We need to define the map

$$f^\sharp : \mathcal{O}_Y \to f_*\mathcal{O}_X.$$

Let U be an open set of $Y = \mathrm{Spec}(R)$ and $g \in \mathcal{O}_Y(U)$. Let $\mathfrak{q} \in (f^*)^{-1}(U)$, which means that $\mathfrak{p} = f^{-1}(\mathfrak{q}) \in U$. Then, by definition, $g([\mathfrak{p}]) \in R_\mathfrak{p}$. But, there is a canonical ring homomorphism $R_\mathfrak{p} \to S_\mathfrak{q}$ induced from the homomorphism $R \to S$. It is simply given by $r/s \mapsto f(r)/f(s)$. Via this homomorphism we may view $g([\mathfrak{p}])$ as an element of $S_\mathfrak{q}$ that we shall call $f^\sharp(g)([\mathfrak{q}])$.

By definition $f^\sharp(g)$ is a function on $f^{-1}(U)$ such that $f^\sharp(g)([\mathfrak{q}]) \in S_\mathfrak{q}$ for all points $[\mathfrak{q}] \in U$. We need to show that this function is locally a fraction. Let $\mathfrak{q}, \mathfrak{p}$ be as before. Then, there is an open set $V \subseteq U$, containing $\mathfrak{p}$ such that on V we have $g = r/s$, where s doesn't belong to any prime ideal $\mathfrak{p}' \in V$. Note then that if $[\mathfrak{q}']$ is such that $f^*([\mathfrak{q}']) = [\mathfrak{p}']$ then $f(s) \notin \mathfrak{q}'$. Under our interpretation of $f^\sharp(g)([\mathfrak{q}'])$, we have that $f^\sharp(g)([\mathfrak{q}'])$ is the image of $g([\mathfrak{p}])$ under $R_{\mathfrak{p}'} \to S_{\mathfrak{q}'}$, namely, the image of r/s, which is $f(r)/f(s)$. Thus, $f^\sharp(g)$ is represented on $f^{-1}(V)$ by $f(r)/f(s)$.

We note that $f^\sharp$ is a morphism of locally ringed spaces. In fact, the induced map on local rings is precisely

$$f\colon R_{\mathfrak{p}} \to S_{\mathfrak{q}},$$

and not only $f^{-1}(\mathfrak{q}) = \mathfrak{p}$ but also $f^{-1}(\mathfrak{q}^e) = \mathfrak{p}^e$, where "e" denotes the extended ideals in the local rings.

It is now easy to check that we got a contravariant functor **Com.Rings** → **Aff.Sch**. By definition it is essentially surjective. It remains to show it is fully-faithful. Taking the open set $U = \mathrm{Spec}(R)$ and $g \in R$ viewed as an element of $\mathcal{O}_X(U)$, per definition the associated element in $\mathrm{Spec}(S) = (f^*)^{-1}(U)$ is simply $f(g)$. Thus, the functor is faithful. It remains to show it is full.

For that we use the following argument, left as an exercise: *if two morphisms $X \to Y$ of locally ringed spaces agree on a collection of open sets that form a basis for Y and their pre-images in X then they are the same morphism.*

We use this principle for the collection $\{D(f) : f \in R\}$ that covers Y. Let $D(h)$ be a basic open set of $Y = \mathrm{Spec}(R)$. Then $(f^*)^{-1}(D(h)) = D(f(h))$ is a basic open set of $\mathrm{Spec}(S)$. We have

$$\mathcal{O}_X(D(h)) = R[h^{-1}].$$

In particular, every function g on $D(h)$ has a *global* representation as r/h^n on $D(h)$. From our definition, $f^\sharp(g) = f(r)/f(h)^n$.

Now, let $(F, F^\sharp)\colon X \to Y$ be any morphism of locally ringed spaces. Then, taking $U = Y = \mathrm{Spec}(R)$ we have a ring homomorphism

$$F^\sharp\colon R = \mathcal{O}_Y(Y) \to S = \mathcal{O}_X(X).$$

Denote this ring homomorphism f. We claim that

$$(f^*, f^\sharp) = (F, F^\sharp).$$

If so, we proved that the functor is full.

Let $\mathfrak{p}$ be a point of X. We have a commutative diagram:

$$\begin{tikzcd}
\mathcal{O}_Y(Y) = R \arrow[r, "f=F^\sharp"] \arrow[d] & F_*\mathcal{O}_X(Y) = S \arrow[d] \\
\mathcal{O}_{Y,F(\mathfrak{p})} \arrow[r, "F^\sharp"] & \mathcal{O}_{X,\mathfrak{p}}
\end{tikzcd}$$

Now, there is a unique way to extend $F^\sharp$ to the localization and so, on the localized rings, we must have $F^\sharp = f$, too. Since the homomorphism of local rings is a local homomorphism, we conclude that in fact

$$F(\mathfrak{p}) = (f)^{-1}(\mathfrak{p}) = f^*(\mathfrak{p}).$$

It follows that for the topological maps we have $F = f^*$. It remains to check that on every open set U of X the map $f^\sharp$ agrees with $F^\sharp$. But it is enough to check that on the basis open sets $U = D(f)$. In this case the rings are again localizations and the argument goes as for the local rings. □

Corollary 16.4.2. *Pullback (fibre product) exists in the category of affine schemes.*

Proof. Given a diagram in **Aff.Sch**

$$\begin{tikzcd} & \mathrm{Spec}(R) \arrow[d] \\ \mathrm{Spec}(S) \arrow[r] & \mathrm{Spec}(A), \end{tikzcd}$$

we have the dual diagram in **Com.Rings**:

$$\begin{tikzcd} & R \\ S & A \arrow[l] \arrow[u] \end{tikzcd}$$

We have *pushouts* in **Com.Rings**:[11]

$$\begin{tikzcd} R \otimes_A S & R \arrow[l] \\ S \arrow[u] & A \arrow[l] \arrow[u] \end{tikzcd}$$

It provides us with *pullback* in **Aff.Sch**

$$\begin{tikzcd} \mathrm{Spec}(R \otimes_A S) \arrow[r] \arrow[d] & \mathrm{Spec}(R) \arrow[d] \\ \mathrm{Spec}(S) \arrow[r] & \mathrm{Spec}(A). \end{tikzcd}$$

□

Note an important point: the point set of $\mathrm{Spec}(R \otimes_A S)$ is not the fibre product of the point sets of $\mathrm{Spec}(R)$ and $\mathrm{Spec}(S)$ over $\mathrm{Spec}(A)$. For example take

$$A = \mathbb{C}, \quad R = \mathbb{C}[x], \quad S = \mathbb{C}[y].$$

Then, as sets

$$\mathrm{Spec}(\mathbb{C}) = [0], \quad \mathrm{Spec}(\mathbb{C}[x]) = \{[0]\} \cup \{[(x-\alpha)] : \alpha \in \mathbb{C}\}.$$

The fibre product as *sets* is therefore $\mathrm{Spec}(\mathbb{C}[x]) \times \mathrm{Spec}(\mathbb{C}[y])$. However, the point $[(x-y)] \in \mathrm{Spec}(\mathbb{C}[x] \otimes_{\mathbb{C}} \mathbb{C}[y]) = \mathrm{Spec}(\mathbb{C}[x,y])$ is not in this product. For an even more outrageous situation, see Exercise 66.

As a matter of notation, given two affine schemes X, Y with morphisms $X \to Z \leftarrow Y$ we will denote the pullback of the diagram, the **fibre product of** X **and** Y **over** Z by

$$X \times_Z Y.$$

[11] It's a hard typographical decision whether to use this diagram or the diagram

$$\begin{tikzcd} A \arrow[r] \arrow[d] & R \arrow[d] \\ S \arrow[r] & R \otimes_A S. \end{tikzcd}$$

16.5. **The functor of points.** Let $X = \mathrm{Spec}(S)$ be an affine scheme. The functor

$$h^X\colon \mathbf{Aff.Sch.} \to \mathbf{Sets}, \qquad h^X(\mathrm{Spec}(R)) := \mathrm{Mor}(\mathrm{Spec}(R), \mathrm{Spec}(S))$$

is called **the functor of points** defined by X.

We are a bit cavalier here. We should have really taken X to be any fixed affine scheme and define

$$h^X(\mathscr{R}) = \mathrm{Mor}_{\mathbf{Aff.Sch}}(X, \mathscr{R})$$

for any affine scheme $\mathscr{R}$. But we allow ourselves this abuse due to the equivalence of categories established in Theorem 16.4.1. To see why this is called the functor of points consider the following case. Suppose that $X = \mathrm{Spec}(S)$ and

$$S = \mathbb{Z}[x_1, \dots, x_n]/\langle f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\rangle.$$

Then

$$\begin{aligned} h^X(\mathrm{Spec}(R)) &= \mathrm{Mor}_{\mathbf{Aff.Sch}}(\mathrm{Spec}(R), \mathrm{Spec}(S)) \\ &= \mathrm{Mor}_{\mathbf{Com.Rings}}(S, R) \\ &= \mathrm{Mor}_{\mathbf{Com.Rings}}(\mathbb{Z}[x_1, \dots, x_n]/\langle f_1, \dots, f_m\rangle, R) \\ &= \{(r_1, \dots, r_n) \in R^n : f_j(r_1, \dots, r_n) = 0, j = 1, \dots, m\} \end{aligned}$$

Namely, $h^X(\mathrm{Spec}(R))$ are the points on the "variety" defined by the equations $f_1 = \cdots = f_m = 0$ with coordinates in R. That is, the solutions to the equations $f_1 = \cdots = f_m = 0$ in the ring R. By Yoneda's lemma, X is characterized up to isomorphism by its functor of points.

Part 6. Exercises

(1) **Final and initial objects in a category.** Let $\mathbf{C}$ be a category. An object A of $\mathbf{C}$ is called **final** (resp. **initial**) if for every object B the set $\mathrm{Mor}_{\mathbf{C}}(B, A)$ (resp., $\mathrm{Mor}_{\mathbf{C}}(A, B)$) is a singleton. For example, if $\mathbf{C} = \mathbf{Gps}$ then the trivial group $\{1\}$ is both an initial and a final object. If there is an initial object that is also a final object then we call it a **zero object**

- Prove that if a final object exists it is unique up to a unique isomorphism. Do the same for initial objects.
- Give an example of category where there is a final object and no initial object, initial object and no final object, no initial object and no final object, initial object and a final object but they are not isomorphic.

(2) Let $\Phi \colon \mathbf{Top} \to \mathbf{Sets}$ be the forgetful functor. Show that Φ has both a right and a left adjoint functor, but that they are not the same.

(3) Let $F \colon \mathbf{AbGps} \to \mathbf{AbGps}$ be the functor sending a group A to $A[2] = \{a \in A : a + a = 0\}$ and $f \colon A \to B$ to $f|_{A[2]} \colon A[2] \to B[2]$. Does this functor has a left adjoint? right adjoint?

(4) Let **Poset** be the category of partially ordered sets. An object in this category is a set S equipped with a relation $\leq$ such that $x \leq x$ for all x, $x \leq y$ and $y \leq z$ implies $x \leq z$, and $x \leq y$ and $y \leq x$ implies $x = y$. A morphism $f \colon (S, \leq) \to (T, \leq)$ is a function $f \colon S \to T$ such that for all $x, y \in S$ such that $x \leq y$, we have $f(x) \leq f(y)$.

To a topological space X we can associate a poset S_X whose elements $U, V, \dots$ are the open sets in X and we say that $U \leq V$ if $U \subseteq V$. Prove that this defines a contravariant functor

$$\mathbf{Top} \to \mathbf{Poset}.$$

Is it full? Is it faithful?

(5) Let R be a commutative ring and A, B, C R-modules. Prove that

$$A \otimes_R (B \otimes_R C) \cong (A \otimes_R B) \otimes_R C.$$

(6) Let $A_R, B_R,_R C$ be R-modules. Prove that $(A \oplus B) \otimes_R C \cong (A \otimes_R C) \oplus (B \otimes_R C)$. If R is commutative deduce that if $A_1, \dots, A_n$ are free R-modules of rank $d_1, \dots, d_n$, then $A_1 \otimes A_2 \otimes \cdots \otimes A_n$ is a free R-module of rank $d_1 d_2 \cdots d_n$.

(7) Write a complete proof of Theorem 2.7.1.

(8) **Clifford Algebras.** Let F be a field of characteristic different than 2, let V be a vector space of finite dimension $n > 0$ over F, and let

$$B \colon V \times V \to F,$$

be an F-bilinear symmetric form. B defines a quadratic form

$$q \colon V \to F, \qquad q(v) = B(v, v),$$

and the formula

$$2B(x, y) = q(x + y) - q(x) - q(y)$$

shows that q determines B. We refer to (V, q) as a **quadratic space**.

The Clifford algebra $C(V, q)$ is constructed as the quotient of the tensor algebra $T^*(V)$ of V, by the two-sided ideal generated by all elements of the form $v \otimes v - q(v)$ for $v \in V$. Thus,

$$C(V, q) = T^*(V) / \langle v \otimes v - q(v) \rangle.$$

Note that $C(V, q)$ is $\mathbb{Z}/2\mathbb{Z}$-graded and the even part $C^0(V, q)$, which is a subalgebra, is called the **even Clifford algebra**.

The case where q is identically 0 is interesting too. In fact, we just get the exterior algebra of V that way! In this exercise we will find a basis for $C(V, q)$.

For $\mathbb{Z}/2\mathbb{Z}$ graded F-algebras A, B,we define a variant of their tensor product $A \otimes_F B$ that we will denote $A \otimes_F^{gr} B$. As an F-vector space $A \otimes_F^{gr} B$ is just $A \otimes_F B$ but the algebra structure is defined as follows: we call an element of A homogenous if $a \in A_0$ or $a \in A_1$ and we put $\partial a = i$ to indicate that $a \in A_i$. The same definition applies for elements of B. Multiplication is then induced by the formula valid for *homogenous elements*

$$(a \otimes b)(a' \otimes b') = (-1)^{\partial b \, \partial a'} aa' \otimes bb',$$

which is the usual multiplication up to a sign. Note though that for calculation this product for general elements $a, a' \in A, b, b' \in B$, one has first to decompose them as a sum of homogenous elements, then apply distributive laws, etc. As

$$A \otimes_F B = (A_0 \otimes_F B_0 \oplus A_1 \otimes_F B_1) \oplus (A_1 \otimes_F B_0 \oplus A_0 \otimes_F B_1),$$

these rules determine the new multiplication on $A \otimes_F B$. We also see that $A \otimes_F^{gr} B$ is a $\mathbb{Z}/2\mathbb{Z}$-graded algebra whose elements of degree 0 are $A_0 \otimes_F B_0 \oplus A_1 \otimes B_1$.

Answer the following questions.

(a) When $\dim(V) = 1$, let v be a non-zero vector. Prove that $C(V, q) \cong F[x]/(x^2 - q(v))$.

(b) We write the product in $C(V, q)$ simply as xy. Prove that

$$xy = -yx + 2B(x, y).$$

In particular, if x, y, are orthogonal then $xy = -yx$, and conversely.

(c) Prove that if W is any F-algebra and $f\colon V \to W$ is a map of F-vector spaces satisfying $f(v)^2 = q(v) \cdot 1_W$, there is a unique homomorphism of F-algebras $C(V, q) \to W$ extending the map on V.

(d) Given two vector spaces $(V_1, q_1), (V_2, q_2)$, their **orthogonal sum** $(V_1 \perp V_2, q_1 \perp q_2)$ is the vector space $V_1 \oplus V_2$ with the quadratic form

$$q((v_1, v_2)) = q_1(v_1) + q(v_2).$$

Using the previous question, prove that there is a surjective homomorphism

$$C(V_1 \perp V_2, q_1 \perp q_2) \to C(V_1) \otimes_{\mathbb{F}}^{gr} C(V_2),$$

such that

$$(v_1, v_2) \mapsto v_1 \otimes 1 + 1 \otimes v_2.$$

(e) Prove, by hand, that if $e_1, \dots, e_n$ is an orthonormal basis for V then

$$\{e_{i_1} e_{i_2} \cdots e_{i_t} : 1 \leq t \leq n, 1 \leq i_1 < i_2 < \cdots < i_t \leq n\}$$

is a spanning set for $C(V, q)$. (The orthonormality assumption is not necessary, but it simplifies the argument.) For example, if $\dim(V) = 1$ and e_1 is a basis then $\{1, e_1\}$ is a spanning set for $C(V, q)$. If $\dim(V) = 2$, then $\{1, e_1, e_2, e_1 e_2\}$ is a spanning set and so on.

(f) Now, combine induction on $\dim(V)$ and the statements you have already proven to show that

$$\dim(C(V, q)) = 2^n,$$

and conclude that $\{e_{i_1} e_{i_2} \cdots e_{i_t} : 1 \leq t \leq n, 1 \leq i_1 < i_2 < \cdots < i_t \leq n\}$ is a basis.

(g) Let (V, q) be a two dimension quadratic space over F with orthogonal basis i, j such that $q(i) = a, q(j) = b$. Then $C(V, q)$ is a quaternion algebra. That is, prove that $C(V, q)$ is isomorphic to the algebra

$$F \oplus Fi \oplus Fj \oplus Fk,$$

where $i^2 = a, j^2 = b, ij = -ji = k$. The case $a = 1, b = 1$ gives $M_2(F)$. Therefore, Clifford algebras are higher dimensional generalizations of quaternion algebras, as well as exterior algebras (the case $q \equiv 0$).

(h) Consider the invertible elements x of $C^0(V,q)$ such that $xvx^{-1} \in V, \forall v \in V$, when we think about V as a subspace of $C(V,q)$. Show that the collection of these elements is a group, called the **general Spin group** $\mathrm{GSpin}(V,q)$ of (V,q). Show that for $x \in \mathrm{GSpin}(V,q)$ the map $v \mapsto xvx^{-1}$ is an orthogonal transformation of V. Conclude that there is a homomorphism

$$\mathrm{GSpin}(V,q) \to \mathrm{O}(V).$$

The image actually lies in $\mathrm{SO}(V)$, but you are not asked to prove that. Also, it turns that the kernel of this homomorphism is precisely $F^\times$ and that the sequence

$$1 \to F^\times \to \mathrm{GSpin}(V,q) \to \mathrm{SO}(V) \to 1,$$

is exact as a sequence of algebraic group. This means that it is exact in the usual sense except that the homomorphism to $\mathrm{SO}(V)$ is not necessarily surjective, but it is always surjective when F is algebraically closed.

The groups GSpin and their relatives Spin are important in physics and in many branches of mathematics.

(9) **Finite Fourier analysis.**[12] Let G be a finite abelian group, $|G| = n$, and $\hat{G} = G^*$ its character group. We make the functions $G \to \mathbb{C}$ into a Hilbert space, denoted $L^2(G)$ by

$$\langle f_1, f_2 \rangle = \frac{1}{n} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

Note that as G is abelian, $L^2(G)$ is just the space of class functions on G, with the same inner product already used. In additive notation for G the characters satisfy

$$\chi(a+b) = \chi(a) \cdot \chi(b).$$

Given a function $f\colon G \to \mathbb{C}$, define its Fourier transform

$$\hat{f}\colon \hat{G} \to \mathbb{C},$$

by

$$\hat{f}(\chi) := \langle f, \chi \rangle = \frac{1}{n} \sum_{g \in G} f(g)\bar{\chi}(g).$$

This provides a linear map $L^2(G) \to L^2(\hat{G})$ that is not quite norm preserving.

(a) Prove the Fourier inversion formula

$$f = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \cdot \chi.$$

(b) Calculate $\hat{\chi}$ for $\chi \in \hat{G}$. Calculate $\hat{\delta}_g$ where $\delta_g\colon G \to \mathbb{C}$, receives the value 1 at g and is otherwise 0.

(c) Prove that $\hat{\hat{f}}(x) = \frac{1}{n} f(-x)$ under the natural identification $\hat{\hat{G}} = G$ (Pontryagin duality) taking $a \in G$ to the character on $\hat{G}$ that takes χ to $\chi(a)$.

(d) Prove Plancherel's formula: $\|\hat{f}\|^2 = \frac{1}{n}\|f\|^2$.

[12] I have done my best to make sure all the constants appearing here are correct. There is no standard normalization of the inner products in the literature and I had to adapt references I was relying on. If you find a mistake, please let me know.

(e) For $a \in G$ (written additively) define the translation by a map T_a as

$$(T_a f)(x) = f(x+a).$$

Prove that

$$\widehat{T_a f}(\chi) = \chi(a)\hat{f}.$$

(f) Define convolution on $L^2(G)$ by

$$(f * g)(x) = \frac{1}{n}\sum_{a \in G} f(x-a)g(a).$$

Prove that $f * g = g * f$ and that

$$\widehat{f * g} = \hat{f} \cdot \hat{g}.$$

(10) **Another model for induced representations.** Let $H < G$ and let (σ, V) be a representation of H. Consider the vector space

$$U = \{f \colon G \to V : f(xh) = \sigma(h)^{-1}f(x), \forall h \in H, x \in G\}.$$

For $g \in G$ and $f \in U$ define a new function $\rho(g)f \colon G \to V$ by

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

Show that this defines a linear representation $\rho : G \to \mathrm{GL}(U)$. Show that there is an isomorphism

$$U \cong \mathrm{Ind}_H^G V.$$

(11) By following the method for the case of odd n, find all the irreducible representations of the dihedral group D_n when n is even.

(12) Prove Corollary 5.9.2.

(13) Let G, H be finite groups. Prove that the isomorphism classes of the irreducible representations of $G \times H$ are precisely of the form $(\rho_G, V_G) \otimes_{\mathbb{C}} (\rho_H, V_H)$, where (ρ_G, V_G) (resp. (ρ_H, V_H)) is an irreducible representation of G (resp. H) and the action is given by

$$\rho(g,h)(v \otimes w) = \rho_G(g)v \otimes \rho_H(h)w.$$

(14) Let $\mathbb{F}$ be a finite field of q elements and B the Borel subgroup of $\mathrm{GL}_2(\mathbb{F})$,

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{F}, ad \neq 0 \right\}.$$

Find all the irreducible representations of B. As follows:

(a) Prove that $B^{ab} \cong \mathbb{F}^\times \times \mathbb{F}^\times$ and identify all the irreducible 1-dimensional representations of B.

(b) Calculate the conjugacy classes of B and conclude that B has $q^2 - q$ irreducible representations.

(c) The subgroup $N < B$ defined by $a = d$ is a normal subgroup. Consider induced representations $\mathrm{Ind}_N^B V$, where V is a 1-dimensional representation of N.

(15) (a) Find the four 1-dimensional representations of the quaternion group Q and calculate for each its character.

(b) The quaternion group Q acts on $\mathbb{C}^2$ via its embedding $Q \subseteq \mathrm{GL}_2(\mathbb{C})$. Write the character χ for this action and calculate $\|\chi\|^2$.

(c) Write the character table of Q.

(16) (a) Find the three 1-dimensional representations of A_4 and calculate for each its character.

(b) The group A_4 acts on $\mathbb{R}^3$ via its action on a regular tetrahedron. Write the character χ for this action and calculate $\|\chi\|^2$. (Hint: you don't have to work with the usual basis. There is a another basis for $\mathbb{R}^3$ in which the computations are much easier!)

(c) Write the character table of A_4.

(17) Find the decomposition of the representation $\mathbb{Z}/4\mathbb{Z} \to \mathrm{GL}_2(\mathbb{C})$, $a \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)^a$ into a sum of irreducible representations.

(18) Up to isomorphism there are 3 non-abelian groups of order 12: A_4, D_6 and a

$$T = \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z},$$

where $1 \in \mathbb{Z}/4\mathbb{Z}$ acts on $\mathbb{Z}/3\mathbb{Z}$ by multiplication by -1. (See MATH 456). Find the character table of T.

(19) Let G be a finite group of order n and class number h and consider its character table. Modify the rows of the character table suitably so as to obtain genuine orthogonal rows and so a $h \times h$ orthogonal matrix. Use this modified matrix to prove that the columns of the character table are orthogonal too and so for $g, h \in G$ and $\{\chi_i\}$ the irreducible characters of G:

$$\sum_{\chi_i} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |\mathrm{Cent}_G(g)|, & \text{if } g, h \text{ are conjugate;} \\ 0, & \text{otherwise.} \end{cases}$$

(The summation extending over the irreducible characters.)

(20) Show that for $n \geq 4$, $\rho^{st,0}$, viewed as a representation of A_n, is irreducible.

(21) Let z be a central element of a finite group G and V an irreducible representation of G. Show that z acts on V as a multiple of the identity endomorphism and that this defines a 1-dimensional character $Z(G) \to \mathbb{C}^\times$, called the **central character** of the representation.

(22) Consider $D_4 = \langle (1234), (24) \rangle$ as a subgroup of S_4.

(a) Prove that D_4 has exactly 3 non-trivial 1-dimensional characters χ, and that they correspond bijectively to its 3 subgroups of order 4 by sending χ to $\mathrm{Ker}(\chi)$.

(b) If χ is such a character and K its kernel, prove that $\mathrm{Ind}_{D_4}^{S_4}\chi$ is an irreducible 3-dimensional representation of D_4, unless $K = V$, the Klein group.

(c) In the case $K = V$, find the decomposition of the induced representation.

(d) Do we get every 3-dimensional irreducible representation of S_4 this way?

(e) Is every irreducible representation of S_4 induced from a 1-dimensional character of a subgroup?

(23) Let (ρ, V) be an irreducible representation of a group G. Show that to give a $\mathbb{C}$-bilinear form on V is equivalent to giving a homomorphism $V \to V^*$. Use Schur's lemma to conclude that if a G invariant form exists, it is unique. Use characters to deduce that a G-invariant form exists if and only if χ_ρ takes real values only. (In the text we have dealt with the finer question of whether a symmetric G-invariant form exists.)

(24) In this exercise we will study the irreducible representations of S_5.

- Prove that S_5 has 7 irreducible represenations.
- By calculating the characters of $\wedge^a \rho^{St,0}$ for $a = 1, 2, 3, 4$, and including also $\mathbb{1}$, we find 5 irreducible representations.
- Conclude that there are two additional irreducible representations and they are both 5-dimensional.
- Decompose the representation $\rho^{St,0} \otimes \rho^{St,0}$ into irreducible representations.
- Complete the character table of S_5

(25) Let $G \subset S_5$ be the subgroup of order 20 generated by the two permutations $c = (12345)$ and $f = (1243)$. Note that $fcf^{-1} = c^2$ and therefore $K = \langle c \rangle$ is a normal subgroup of G and $H = \langle f \rangle$ is a subgroup such that $H \cap K = \{1\}$. Find the irreducible representations of G.

Remark 16.5.1. The group G is an example of a **Frobenius group**: it is a group acting transitively on a set (in our case $\{1, 2, 3, 4, 5\}$) such that any non-trivial element of G has at most 1 fixed point and there is a non-trivial element with exactly one fixed point (in our case, (1243)). Then, quite generally,

$$G = H \ltimes K,$$

where H is the stabilizer of a chosen element of the set (in our case, the element 5) and K consists of the identity element and the elements of G that do not fix any element of the set S. In general, it is not clear at all, and the only proof uses character theory, that K is a subgroup of G. Clearly K is normal. In our case, a calculation gives that $K = \langle c \rangle$ which is clearly a subgroup.

(26) Use Frobenius' formula for the character of V_λ to deduce the hook length formula. (This exercise, taken from Fulton and Harris, looks reasonable, but it may be nasty. I haven't tried.)

(27) Use the hook length formula to prove that the only irreducible representations of S_n of dimension less that n are $\mathbb{1}, \mathrm{sgn}, \rho^{St,0}$ and $\rho^{St,0} \otimes \mathrm{sgn}$. Find the Young diagrams corresponding to these representations (see examples in the text). (Same comments as for Exercise 26, although this one looks a bit simpler, at first sight.)

(28) What is the connection between V_λ and $V_{\lambda'}$ where λ and λ' are conjugate tableaux?

(29) Prove the statement made in Example 8.2.9 concerning the Young diagram of the representation $\wedge^a \rho^{St,0}$. A proof just for the case $a = 2$ would also be acceptable.

(30) **Opposite category.** Let $\mathbf{C}$ be a category. Define the **opposite category**, also called the **dual category**, $\mathbf{C}^{\mathrm{op}}$ as follows. The objects of $\mathbf{C}^{\mathrm{op}}$ are the same as the objects of $\mathbf{C}$, but for any two objects A, B we define

$$\mathrm{Mor}_{\mathbf{C}^{\mathrm{op}}}(A, B) := \mathrm{Mor}_{\mathbf{C}}(B, A).$$

(a) Prove that $\mathbf{C}^{\mathrm{op}}$ is a category.
(b) Prove that if $F\colon \mathbf{C} \to \mathbf{D}$ is a covariant/contravariant functor then it defines a functor $F^{\mathrm{op}}\colon \mathbf{C}^{\mathrm{op}} \to \mathbf{D}$ that is contravariant/covariant, respectively.
(c) Prove that $h_{X,\mathbf{C}^{\mathrm{op}}} = h^{X,\mathbf{C}}$ (see § 10).
(d) Prove that if X is an initial/final object of $\mathbf{C}$, it is a final/initial object of $\mathbf{C}^{\mathrm{op}}$.
(e) Recall that to a group G we associate a category $*_G$. Is the opposite category $*_G^{\mathrm{op}}$ also of the form $*_H$ for some H? Show that if G is abelian then $*_G \cong *_G^{\mathrm{op}}$. Is this the only case?

(31) Consider the following functors. Determine if they are representable.
(a) The forgetful functor ${}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{Sets}$, where R is a ring.
(b) The forgetful functor $\mathbf{Rings} \to \mathbf{Sets}$, where $\mathbf{Rings}$ is the category of rings (and a ring homomorphism must take 1 to 1).
(c) The functor $\star\mathbf{Top}' \to \mathbf{Sets}$ associating to a locally-connected, locally path-connected pointed topological space (X, x_0) its fundamental group $\pi_1(X, x_0)$ thought of as a set only. (So, it is really the composition $\star\mathbf{Top}' \to \mathbf{Gps} \to \mathbf{Sets}$, where the forgetful functor is composed with the functor π_1.)
(d) The functor $\mathbf{Gps} \to \mathbf{Sets}$ taking a group A to the set $A^n = A \times A \times \cdots \times A$, where n is some fixed positive integer.

(32) We defined the properties "full", "faithful" and "essentially surjective". A functor may or may not have these properties, giving us 8 possibilities. Provide an example for each.

(33) Let k be a field and define a category $\mathbf{C}$, whose objects are $\{0\}, k, k^2, k^3, \dots$. The morphisms are

$$\mathrm{Mor}(k^a, k^b) = M_{b,a}(k),$$

the $b \times a$ matrices with entries in k and composition is provided by product of matrices. On the other hand, let $\mathbf{D}$ be the category of finite dimensional k-vector spaces. Prove that $\mathbf{C}$ and $\mathbf{D}$ are equivalent categories.

(34) Referring to § 11.2.1, let $L = K[t]/(t^2 - a)$. It is a commutative ring containing K with an involution $x + yt \mapsto x - yt$ that we denote $\alpha \mapsto \bar{\alpha}$, $\alpha \in L$. Consider the matrices in $M_2(L)$ given by

$$\left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in L \right\}.$$

Prove that this is a ring that is a model for the quaternion algebra $\left(\frac{a,b}{k}\right)$ (If we denote $[\alpha, \beta]$ such matrix, consider $[1,0], [t,0], [0,1], [0,t]$) and the norm map corresponds to the determinant. Conclude the statements $N(u) = u\bar{u}, N(u_1u_2) = N(u_1)N(u_2)$ and that an element is invertible if and only if its norm is non-zero (it is also easy to prove these directly by calculation).

(35) Consider the Hamilton quaternion $\mathbb{H}$ and the subspace

$$S^2 = \{xi + yj + zk : x, y, z \in \mathbb{R}, x^2 + y^2 + z^2 = 1\}$$

that we can identify it with the 2-dimensional sphere in $\mathbb{R}^3$.

(a) Prove that there is a group action of $\mathbb{H}^\times$ on S^2, where $h \in \mathbb{H}, h \neq 0$ acts on $p \in S^2$ by

$$p \mapsto hph^{-1}.$$

(b) Prove that this in fact produces an injection

$$\mathbb{H}^\times/\mathbb{R}^\times \to O_3(\mathbb{R}),$$

where $O_3(\mathbb{R})$ is the group of orthogonal 3×3 matrices.

(c) Prove that in fact,

$$\mathbb{H}^\times/\mathbb{R}^\times \to SO_3(\mathbb{R}).$$

(Use a topological argument, if convenient.)

(d) Prove that there is an isomorphism

$$\mathbb{H}^\times/\mathbb{R}^\times \cong SO_3(\mathbb{R}).$$

(I don't know if there is an easy proof without using something from the theory of algebraic groups, or Lie groups. One can give a more pedestrian proof by first proving that $\mathbb{H}^\times$ contains all rotations fixing the point $i \in S^2$ (and similarly for j and k), and using this to show also that $\mathbb{H}^\times$ acts transitively on S^2. At the same time, one proves that $SO_3(\mathbb{R})$ is generated by rotations around fixed vectors.)

This gives a very compact representation for rotations. Instead of exhibiting them as 3×3 matrices, which requires 9 parameters, we can represent them as quaternions of the form $1 + ai + bj + ck$ and that requires only 3 parameters. Instead of multiplying 2 matrices which will require 27 multiplications, we can multiply quaternions (and renormalize them) which will require 9 multiplication and 1 division. This is used in video games and flight simulators to speed up performance.

(36) Let m, n be positive integers. Let R be a division algebra. Prove that there is a ring homomorphism

$$M_m(R) \to M_n(R)$$

if and only if $m|n$.

(37) Let I be a directed poset and $\{X_i, f_{ij}\}$ a direct system of sets indexed by I. Define a set S whose elements are equivalence classes $[(i, x_i)]$ where $(i, x_i) \sim (j, x_j)$ if there exists a k such that $i \leq k, j \leq k$ and $f_{ik}(x_i) = f_{jk}(x_j)$. Prove that this is indeed an equivalence relation and that S with the natural maps $X_i \to S$, $x_i \mapsto [(i, x_i)]$, is the direct limit.

(38) Let I be a directed poset and $\{R_i, f_{ij}\}$ a direct system of rings indexed by I.
  (a) Prove that the direct limit $\varinjlim R_i$ exists in the category of rings. (Try to define it using a description of the direct limit as in Exercise 37, now endowed with suitable addition and multiplication rules.)
  (b) Let R_i be the ring of complex analytic functions on the open disc $|z| < 1/i$ around 0. For $i < j$ the natural restriction may $R_i \to R_j$ is injective. Find a description in terms of power series of the limit ring $\varinjlim R_i$. (This requires some knowledge of basic complex analysis.)

(39) Prove that the coproduct of two commutative rings R, S, exists in the category of commutative rings and is given by $R \otimes_{\mathbb{Z}} S$.

(40) Prove that pushouts exist in the category of commutative rings.

(41) Consider pushout in the category $_{\mathbf{R}}\mathbf{Mod}$

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \\
C &
\end{tikzcd}$$

Prove that the pushout affords the description

$$B \oplus C/W,$$

where W is the R submodule generated by $\{(f(a), -g(a)) : a \in A\}$.

(42) Prove that $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ is an infinite group by mapping it to a group with two "highly non-commuting" elements of order 2. Let us denote this group by $\langle g \rangle * \langle h \rangle$, where $g^2 = 1, h^2 = 1$. In fact, if you made a good choice for the first part, you will find that the image of the element gh is of infinite order. (Those that know topology well may enjoy finding a topological space with $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ as a fundamental group).

(43) Let $\mathbf{C}$ be a category where both pushouts and pullbacks exists. Suppose that

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \arrow[d] \\
C \arrow[r] & D
\end{tikzcd}$$

is a pushout diagram. Is it the case that A is the pullback?

(44) Let A, B, C be topological spaces and let $f\colon A \to C, g\colon B \to C$ be continuous maps. Prove that the diagram

$$\begin{tikzcd} & A \arrow[d, "f"] \\ B \arrow[r, "g"] & C \end{tikzcd}$$

has a pullback which is the set $\{(a,b) \in A \times B : f(a) = g(b)\}$, endowed with the topology induced from the product topology. It is denoted $A \times_C B$.

Give an example where A and B are connected but $A \times_C B$ is not.

(45) Given a p-adic number $x \in \mathbb{Z}_p$ define its valuation

$$\mathrm{val}(x) = \max\{n : x \in p^n\mathbb{Z}_p\}.$$

Given two p-adic numbers $a, b \in \mathbb{Z}_p$ define

$$d(a,b) = p^{-\mathrm{val}(a-b)}.$$

(a) Prove that $d(a,b)$ is a metric on $\mathbb{Z}_p$ inducing the same topology on $\mathbb{Z}_p$ coming from its description as an inverse limit. It satisfies the non-archemedian triangle inequality

$$d(a,b) \leq \max\{d(a,c), d(b,c)\}.$$

(b) Prove that $\mathbb{Z}_p$ is complete relative to this metric and that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Consequently, $\mathbb{Z}_p$ is the metric completion of $\mathbb{Z}$. (It may be convenient to express elements of $\mathbb{Z}_p$ as infinite sums $\sum_{i=0}^{\infty} a_i p^i$, where $a_i \in \{0, 1, \dots, p-1\}$.)

(c) Let $\mathbb{Q}_p$ be the fraction field of $\mathbb{Z}_p$ then $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$ and the same formula for $\mathrm{val}(x)$ extends it to $\mathbb{Q}_p$; $d(a,b)$ extends to $\mathbb{Q}_p$ as well and $\mathbb{Q}_p$ is the metric completion of $\mathbb{Q}$ relative to this metric.

(46) Let $R = \mathbb{Z}[x]$ and p a prime number. Consider the ideals I, J, K, where $I = \langle p \rangle$, $J = \langle x \rangle$ and $K = \langle p, x \rangle$. Find the completion of R relative to these 3 ideals.

(47) Consider the ring $R = \mathbb{C}[x,y]/(y^2 - x^2(x+1))$ and the ideal $I = \langle x, y \rangle$. Prove that the completion of R relative to I is isomorphic to the ring $\mathbb{C}[\![s,t]\!]/(st)$.

(48) Let $F\colon \mathbf{C} \to \mathbf{D}$ be a covariant functor, and let $G\colon \mathbf{D} \to \mathbf{C}$ be a covariant functor such that (F, G) are an adjoint pair.

(a) Prove that F takes direct limits to direct limits. Namely, if $\{X_i, f_{ij}\}$ is a direct system in $\mathbf{C}$ that has a direct limit $\varinjlim X_i$ then $\{FX_i, Ff_{ij}\}$ is a direct system in $\mathbf{D}$ with a direct limit $F\varinjlim X_i$.

(b) Prove that G takes inverse limits to inverse limits.

(c) Write down the consequence for the functors $M \otimes_R$, $\mathrm{Hom}_R(M, \cdot)$, and the forgetful functor Φ : **Gps** → **Sets**.

(49) Find the injective and projective limit of the diagram of R-modules $\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \end{tikzcd}$, given that $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

(50) Posets form a category **Posets** whose objects are posets and whose morphism are functions that respect order ($i \leq j \Rightarrow f(i) \leq f(j)$). Similarly, **linearly ordered sets**, that is, posets I in which for every i, j in I either $i \leq j$ or $j \leq i$ form a category **losets** (which is a full subcategory of **Posets**). Prove that in the category of linearly ordered sets co-products $A \coprod B$ need not exist, but that co-products $A \coprod B$ exist in the category of posets.

(51) Consider the following system of $\mathbb{Z}$-modules:

(a) $\dots \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z} \to \dots$

(b) $\dots \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}$.
(c) $\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z} \to \dots$

In each case, all arrows are multiplication by a fixed prime p. Find in each case the direct and projective limit of the system.

(52) Give an example of a category that doesn't have projective limits.

(53) Let A, B be groups. Prove that $(A * B)^{ab} \cong A^{ab} \oplus B^{ab}$.

Let R be a commutative ring. The following exercises (54) - (57) examine the notion of "local properties". These are properties that hold true if and only if they are true for all localizations at prime ideals of R.

(54) (Being zero is a local property). Let R be a commutative ring and let M be an R module. Prove that $M = 0$ if and only if $M_{\mathfrak{p}} = 0$ for all primes $\mathfrak{p}$ of R. (If $M \neq 0$, choose a non-zero $m \in M$ and consider a maximal ideal containing the ideal $Ann(m) = \{r \in R : rm = 0\}$.)

(55) (Exactness is a local property). Let R be a commutative ring and let

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "f"] & M_2 \arrow[r, "g"] & M_3 \arrow[r] & 0, \end{tikzcd}$$

be a complex of R-modules. That only means that $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$ and nothing more. Prove that this sequence is a short exact sequence if and only if for all prime ideals $\mathfrak{p} \lhd R$ the sequence

$$\begin{tikzcd} 0 \arrow[r] & M_{1,\mathfrak{p}} \arrow[r, "f"] & M_{2,\mathfrak{p}} \arrow[r, "g"] & M_{3,\mathfrak{p}} \arrow[r] & 0 \end{tikzcd}$$

is short exact.

(56) (Free is not a local property). Let R be a commutative ring.
(a) Prove that the forgetful functor $\Phi\colon {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{Sets}$ has a left adjoint. Namely, for a set X there is an R-module $M(X)$ with the property

$$\mathrm{Hom}_{{}_{\mathbf{R}}\mathbf{Mod}}(M(X), N) \cong \mathrm{Mor}_{\mathbf{Sets}}(X, N).$$

And, if fact, show that we may take $M(X) = \oplus_{x \in X} R$. Namely, that it is the direct sum of copies of R indexed by the discrete poset X. An R-module is called **free** if it is isomorphic to $M(X)$ for some set X.
(b) Let $R = \mathbb{Z}[\sqrt{-6}]$ and $I = \langle 2, \sqrt{-6} \rangle$.
(i) Prove that I is not a free R-module. It is not even of the form Rb for some $b \in R$.
(ii) Prove that I is a prime ideal; in fact, the only prime ideal of R that contains 2.
(iii) Prove that $I_{\mathfrak{p}} = R_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p} \neq I$ of R.
(iv) Prove that $I_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module when $I = \mathfrak{p}$. (Make use of the element $\frac{2}{\sqrt{-6}} = \frac{-\sqrt{-6}}{3}$.)
(v) Conclude that I is a locally free ideal that is not free. Thus, being free is not a local property.
(vi) Note that I is a locally cyclic R-module but is not globally cyclic. Thus, begin cyclic is likewise not a local property.

(57) (Being a domain is not local property). Let k be a field. Prove that $R = k \times k$ is not an integral domain but the localization $R_{\mathfrak{p}}$ is an integral domain for every prime ideal $\mathfrak{p}$ of R.

(58) Let R be a commutative ring and $\mathfrak{p}$ a prime ideal of R. Prove that $V(\mathfrak{p}) \subseteq \mathrm{Spec}(R)$ is the closure of the point $[\mathfrak{p}]$.

(59) Let R be a commutative ring. Prove that $\mathrm{Spec}(R)$ is disconnected if and only if $R \cong R_1 \times R_2$, a direct product of two commutative rings.

(60) Draw and describe the schemes Spec $\mathbb{Q}[x]/(x^n - 1)$, Spec $\mathbb{C}[x]/(x^n - 1)$ and the morphism

$$\mathrm{Spec}\ \mathbb{C}[x]/(x^n - 1) \to \mathrm{Spec}\ \mathbb{Q}[x]/(x^n - 1)$$

coming from the inclusion of rings $\mathbb{Q}[x]/(x^n - 1) \hookrightarrow \mathbb{C}[x]/(x^n - 1)$.

(61) Let R be a commutative ring and $\{f_\alpha : \alpha \in A\}$ a set of elements of R. Then $\mathrm{Spec}(R) = \cup_\alpha D(f_\alpha)$ if and only if $\langle \{f_\alpha : \alpha \in A\} \rangle$, the ideal generated by all the f_α, is equal to R. (Note that we can rephrase $\mathrm{Spec}(R) = \cup_\alpha D(f_\alpha)$ by $\mathrm{Spec}(R) = \cup_\alpha \mathrm{Spec}(R[f_\alpha^{-1}])$, but that is not needed for the solving the exercise.)

(62) Use Exercise 61 to prove that $\mathrm{Spec}(R)$ is compact – every open cover has a finite subcover.

(63) Let R be a commutative ring. Prove that R is a local ring if and only if it has an ideal $\mathfrak{m} \neq R$ such that every element of $R - \mathfrak{m}$ is a unit.

(64) Let R be a commutative ring. Prove that $\mathrm{Spec}(R)$ consists of a single point if and only if R is a local ring and every element of its maximal ideal is nilpotent. Provide examples of such rings.

(65) Let R be a commutative ring and $f \in R$. Prove that $D(f)$ is the empty set if and only if f is nilpotent.

(66) Let k be a field and let s, t, be free variables. Then $k, k(s)$ and $k(t)$ are all fields and therefore $\mathrm{Spec}(k), \mathrm{Spec}(k(s))$ and $\mathrm{Spec}(k(t))$ are all one point spaces. Discuss the scheme

$$\mathrm{Spec}(k(s) \otimes_k k(t)).$$

In particular, show that it has "many many" points.

additional exercises

(67) The affine schemes $\mathrm{Spec}(\mathbb{Q}), \mathrm{Spec}(\mathbb{Q}(i))$ are one point spaces and there is a natural morphism $\mathrm{Spec}(\mathbb{Q}(i)) \to \mathrm{Spec}(\mathbb{Q})$. Describe the fibre product $\mathrm{Spec}(\mathbb{Q}(i)) \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\mathbb{Q}(i))$: determine the underlying set, its topology, the value of the sheaf on each open set and the local rings.

Generalize to $\mathrm{Spec}(K) \times_{\mathrm{Spec}(L)} \mathrm{Spec}(K)$ for $K \supseteq L$ a Galois extension of fields.

(68) Let

$$\begin{tikzcd} & Y \arrow[d] \\ X \arrow[r] & Z \end{tikzcd}$$

be a diagram of affine schemes. We may also view it as a diagram of topological spaces. We can thus take the fibre product in each of these categories. We will denote the fibre product as schemes (temporarily) $X \overset{\mathbf{Sch}}{\times}_Z Y$ and the fibre product as topological spaces by $X \overset{\mathbf{Top}}{\times}_Z Y$. Prove that there is a map of topological spaces

$$X \overset{\mathbf{Sch}}{\times}_Z Y \to X \overset{\mathbf{Top}}{\times}_Z Y,$$

but that in general it is not an isomorphism.

(69) Let A be a ring. An **involution** on A is a map $\sigma\colon A \to A$, $a \mapsto \sigma(a) =: \bar{a}$, which is an antiautomorphism of order ≤ 2. Meaning:

$$\overline{(a+b)} = \bar{a} + \bar{b}, \;\; \overline{ab} = \bar{b}\bar{a}, \;\; \bar{1} = 1, \bar{\bar{a}} = a, \quad \forall a, b \in A.$$

Examples include $\sigma = id_A$ if A is commutative, complex conjugation on $\mathbb{C}$, $x \mapsto \bar{x}$ on a quaternion algebra, $M \mapsto^t M$ for $M \in M_n(R)$ (any ring R).

(a) Define a ring A^{op} whose elements are $\{a^{op} : a \in A\}$ and where

$$a^{op} + b^{op} := (a+b)^{op}, \quad a^{op}b^{op} = (ba)^{op}.$$

Prove that to give an involution is to give a ring homomorphism $\sigma : A \to A^{op}$ such that $\sigma^2 = id_A$ (where σ is defined on A^{op} the obvious way).

(b) Let A be any ring. Prove that $H(A) = A \times A^{op}$ has a canonical involution given by

$$(a, b^{op}) \mapsto (b, a^{op}).$$

(c) Prove that $A \mapsto H(A)$ is a functor **Rings** $\to$ **Inv**.**Rings**, for the category of rings to the category of rings with involution (there is an obvious definition of the latter – state it!), which is right adjoint to the forgetful functor **Inv**.**Rings** $\to$ **Rings**.

(d) Let (A, σ) be a semisimple ring with involution. We can decompose A as a product $A_1 \times \cdots \times A_n \times B_1 \times \cdots \times B_m$, where the A_i are simple and $\sigma(A;_i) = A_i$ and each B_j is the products of two simple algebras $C_j \times D_j$ with $\sigma(C_j) = D_j$. The rings B_j are isomorphic to hyperbolic rings, $B_j \cong H(C_j)$. A ring such as A_i of B_j are called a simple ring with involution as it cannot be decomposed with the involution.

INDEX