# ALGEBRA: LECTURE NOTES

JENIA TEVELEV

CONTENTS

## §1. Categories and Functors

§1.1. **Categories.** Most mathematical theories deal with situations when there are some maps between objects. The set of objects is usually somewhat static (and so boring), and considering maps makes the theory more

dynamic (and so more fun). Usually there are some natural restrictions on what kind of maps should be considered: for example, it is rarely interesting to consider any map from one group to another: usually we require this map to be a homomorphism.

The notion of a category was introduced by Samuel Eilenberg and Saunders MacLane to capture situations when we have both objects and maps between objects (called morphisms). This notion is slightly abstract, but extremely useful. Before we give a rigorous definition, here are some examples of categories:

EXAMPLE 1.1.1.

- The category **Sets**: objects are sets, morphisms are arbitrary functions between sets.
- **Groups**: objects are groups, morphisms are homomorphisms.
- **Ab**: objects are Abelian groups, morphisms are homomorphisms.
- **Rings**: objects are rings, morphisms are homomorphisms of rings. Often (for example in this course) we only consider commutative rings with identity.
- **Top**: topological spaces, morphisms are continuous functions.
- **Mflds**: objects are smooth manifolds, morphisms are differentiable maps between manifolds.
- $\mathbf{Vect}_k$: objects are $k$-vector spaces, morphisms are linear maps.

Notice that in all these examples we can take compositions of morphisms and (even though we rarely think about this) composition of morphisms is associative (because in all these examples morphisms are functions with some restrictions, and composition of functions between sets is certainly associative). The associativity of composition is a sacred cow of mathematics, and essentially the only axiom required to define a category:

DEFINITION 1.1.2. A category $C$ consists of the following data:

- The set of objects $\mathbf{Ob}(C)$. Instead of writing "$X$ is an object in $C$", we can write $X \in \mathbf{Ob}(C)$, or even $X \in C$.
- The set of morphisms $\mathbf{Mor}(C)$. Each morphism $f$ is a morphism *from* an object $X \in C$ *to* an object $Y \in C$. More formally, $\mathbf{Mor}(C)$ is a disjoint union of subsets $\mathbf{Mor}(X, Y)$ over all $X, Y \in C$. It is common to denote a morphism by an arrow $X \xrightarrow{f} Y$.
- There is a composition law for morphisms
$$\mathbf{Mor}(X, Y) \times \mathbf{Mor}(Y, Z) \to \mathbf{Mor}(X, Z), \qquad (f, g) \mapsto g \circ f$$
which takes $X \xrightarrow{f} Y$ and $Y \xrightarrow{g} Z$ to the morphism $X \xrightarrow{g \circ f} Z$.
- For each object $X \in C$, we have an *identity morphism* $X \xrightarrow{\mathrm{Id}_X} X$.

These data should satisfy the following basic axioms:

- The composition law is associative.
- The composition of any morphism $X \xrightarrow{f} Y$ with $X \xrightarrow{\mathrm{Id}_X} X$ (resp. with $Y \xrightarrow{\mathrm{Id}_Y} Y$) is equal to $f$.

Here is another example.

EXAMPLE 1.1.3. Let $G$ be a group. Then we can define a category $C$ with just one object (let's denote it by $O$) and with

$$\mathbf{Mor}(C) = \mathbf{Mor}(O, O) = G.$$

The composition law is just the composition law in the group and the identity element $\mathrm{Id}_O$ is just the identity element of $G$.

DEFINITION 1.1.4. A morphism $X \xrightarrow{f} Y$ is called an *isomorphism* if there exists a morphism $Y \xrightarrow{g} X$ (called an inverse of $f$) such that

$$f \circ g = \mathrm{Id}_Y \qquad \text{and} \qquad g \circ f = \mathrm{Id}_X .$$

In the example above, every morphism is an isomorphism. Namely, an inverse of any element of $\mathbf{Mor}(C) = G$ is its inverse in $G$.

A category where any morphism is an isomorphism is called a *groupoid*, because any groupoid with one object can be obtained from a group $G$ as above. Indeed, axioms of the group (associativity, existence of a unit, existence of an inverse) easily translate into axioms of the groupoid (associativity of the composition, existence of an identity morphism, existence of an inverse morphism).

Of course not any category with one object is a groupoid and not any groupoid has one object.

EXAMPLE 1.1.5. Fix a field $k$ and a positive integer $n$. We can define a category $C$ with just one object (let's denote it by $O$) and with

$$\mathbf{Mor}(C) = \mathrm{Mat}_{n,n} .$$

The composition law is given by the multiplication of matrices. The identity element $\mathrm{Id}_O$ is just the identity matrix. In this category, a morphism is an isomorphism if and only if the corresponding matrix is invertible.

Here is an example of a category with a different flavor:

EXAMPLE 1.1.6. Recall that a *partially ordered set*, or a *poset*, is a set $I$ with an order relation $\preceq$ which is

- reflexive: $i \preceq i$ for any $i \in I$,
- transitive: $i \preceq j$ and $j \preceq k$ implies $i \preceq k$, and
- anti-symmetric: $i \preceq j$ and $j \preceq i$ implies $i = j$.

For example, we can take the usual order relation $\leq$ on real numbers, or divisibility relation $a|b$ on natural numbers ($a|b$ if $a$ divides $b$). Note that in this last example not any pair of elements can be compared.

Interestingly, we can view any poset as a category $C$. Namely, $\mathbf{Ob}(C) = I$ and for any $i, j \in I$, $\mathbf{Mor}(i, j)$ is an empty set if $i \not\preceq j$ and $\mathbf{Mor}(i, j)$ is a set with one element if $i \preceq j$. The composition of morphisms is defined using transitivity of $\preceq$: if $\mathbf{Mor}(i, j)$ and $\mathbf{Mor}(j, k)$ is non-empty then $i \preceq j$ and $j \preceq k$, in which case $i \preceq k$ by transitivity, and therefore $\mathbf{Mor}(i, k)$ is non-empty. In this case $\mathbf{Mor}(i, j)$, $\mathbf{Mor}(j, k)$, and $\mathbf{Mor}(i, k)$ consist of one element each, and the composition law $\mathbf{Mor}(i, j) \times \mathbf{Mor}(j, k) \to \mathbf{Mor}(i, k)$ is defined in a unique way.

Notice also that, by reflexivity, $i \preceq i$ for any $i$, hence $\mathbf{Mor}(i, i)$ contains a unique morphism: this will be our identity morphism $\mathrm{Id}_i$.

Here is an interesting example of a poset: let $X$ be a topological space. Let $I$ be the set of open subsets of $X$. This is a poset, where the order relation is the inclusion of open subsets $U \subset V$. The corresponding category can be denoted by $\mathbf{Top}(X)$.

§1.2. **Functors.** If we want to consider several categories at once, we need a way to relate them! This is done using functors.

DEFINITION 1.2.1. A covariant (resp. contravariant) functor $F$ from a category $C$ to a category $D$ is a rule that, for each object $X \in C$, associates an object $F(X) \in D$, and for each morphism $X \xrightarrow{f} Y$, associates a morphism $F(X) \xrightarrow{F(f)} F(Y)$ (resp. $F(Y) \xrightarrow{F(f)} F(X)$). Two axioms have to be satisfied:

- $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$ for any $X \in C$.
- $F$ preserves composition: for any $X \xrightarrow{g} Y$ and $Y \xrightarrow{f} Z$, we have $F(f \circ g) = F(f) \circ F(g)$ (if $F$ is covariant) and $F(f \circ g) = F(g) \circ F(f)$ (if $F$ is contravariant).

EXAMPLE 1.2.2. Let's give some examples of functors.

- Inclusion of a subcategory, for example we have a functor

$$\mathbf{Ab} \to \mathbf{Groups}$$

  that sends any Abelian group $G$ to $G$ (considered simply as a group) and that sends any homomorphism $G \xrightarrow{f} H$ of Abelian groups to $f$ (considered as a homomorphism of groups).
- More generally, we have all sorts of *forgetful* covariant functors $C \to D$. This simply means that objects (and morphisms) of $C$ are objects (and morphisms) of $D$ with some extra data and some restrictions on this data. The forgetful functor simply 'forgets' about this extra data. For example, there is a forgetful functor $\mathbf{Vect}_k \to \mathbf{Sets}$ that sends any vector space to the set of its vectors and that sends any linear map to itself (as a function from vectors to vectors). Here we 'forget' that we can add vectors, multiply them by scalars, and that linear maps are linear!
- Here is an interesting contravariant functor: the duality functor $\mathbf{Vect}_k \to \mathbf{Vect}_k$ sends any vector space $V$ to the vector space $V^*$ of linear functions on $V$. A linear map $L : V \to U$ is sent to a contragredient linear map $L^* : U^* \to V^*$ (which sends a linear function $f \in U^*$ to a linear function $v \mapsto f(L(v))$ in $V^*$).
- A very important contravariant functor is a functor $\mathbf{Top} \to \mathbf{Rings}$ that sends any topological space $X$ to its ring of continuous functions $C^0(X, \mathbb{R})$ and that sends any continuous map $X \xrightarrow{f} Y$ to a *pull-back homomoprhism* $f^* : C^0(Y, \mathbb{R}) \to C^0(X, \mathbb{R})$ (just compose a function on $Y$ with $f$ to get a function on $X$).
- Here is an interesting variation: let's fix a topological space $X$ and consider a functor $\mathbf{Top}(X) \to \mathbf{Rings}$ that sends any open subset $U \subset X$ to continuous functions $C^0(U, \mathbb{R})$ on $U$. For any inclusion $U \subset V$ of open sets, the pull-back homomorphism $C^0(V, \mathbb{R}) \to$

$C^0(U, \mathbb{R})$ is just restriction: we restrict a function on $V$ to a function on $U$. This functor $\mathbf{Top}(X) \to \mathbf{Rings}$ is an example of a *sheaf*.

§1.3. **Equivalence of Categories.** It is tempting to consider a category of all categories with functors as morphisms! Indeed, we can certainly define a composition of two functors $C \xrightarrow{F} D$ and $D \xrightarrow{G} E$ in an obvious way, and we have obvious identity functors $C \xrightarrow{\mathrm{Id}_C} C$ that do not change either objects or morphisms. There are some slight set-theoretic issues with this super-duper category, but we are going to ignore them.

However, one interesting issue here is when should we consider two categories $C$ and $D$ as equivalent? An obvious approach is to say that $C$ and $D$ are isomorphic categories if there exist functors $C \xrightarrow{F} D$ and $D \xrightarrow{G} C$ that are inverses of each other. However, this definition is in fact too restrictive. Here is a typical example why:

EXAMPLE 1.3.1. Let $D$ be a category of finite-dimensional $k$-vector spaces and let $C$ be its subcategory that has one object for each dimension $n$, namely the standard vector space $k^n$ of column vectors.

Notice that $\mathbf{Mor}(k^n, k^m)$ can be identified with matrices $\mathrm{Mat}_{m,n}$ in the usual way of linear algebra. The categories $C$ and $D$ are not isomorphic, because $D$ contains all sorts of vector spaces in each dimension, and $C$ contains just one $k^n$. However, the main point of linear algebra is that $C$ is somehow enough to do any calculation, because any $n$-dimensional vector space $V$ is isomorphic to $k^n$ "after we choose a basis in $V$".

Should we consider $C$ and $D$ as equivalent categories? To formalize this, we give the following definition:

DEFINITION 1.3.2. A covariant functor $C \xrightarrow{F} D$ is called an *equivalence of categories* if

- $F$ is essentially surjective, i.e. any object in $D$ is isomorphic (but not necessarily equal!) to an object of the form $F(X)$ for some $X \in C$.
- $F$ is fully faithful, i.e.

$$\mathbf{Mor}_C(X, Y) = \mathbf{Mor}_D(F(X), F(Y))$$

for any objects $X, Y \in C$.

For example, let's return to "linear-algebra" categories above. We have an obvious inclusion functor $F : C \to D$. We claim that $F$ is an equivalence of categories. To show that $F$ is essentially surjective, take $V \in D$, i.e. $V$ is an $n$-dimensional vector space. Then $V$ is isomorphic to $k^n$, indeed any choice of a basis $e_1, \dots, e_n \in V$ gives an isomorphism $V \to k^n$ which sends $v \in V$ to the column vector of its coordinates in the basis $\{e_i\}$. (an act of choice stipulates that we allow the axiom of choice, but let's not worry about such things). This shows that $F$ is essentially surjective. Notice that $F$ is fully faithful by definition: linear maps from $k^n$ to $k^m$ are the same in categories $C$ and $D$. So $F$ is an equivalence of categories.

Our definition has a serious flaw: it is not clear that equivalence of categories is an equivalence relation! We postpone the general statement to exercises, and here just look at our example: is there an equivalence of

categories from $D$ to $C$? We need a functor $G$ from $D$ to $C$. For any $n$-dimensional vector space $V$, there is only one candidate for $G(V)$: it must be $k^n$. Are we done? No, because we also have to define $G(L)$ for any linear map $L : V \to U$. So essentially, we need a matrix of $L$. This shows that there is no canonical choice for $G$: unlike $F$, $G$ is not unique. However, we can do the following: let's choose a basis in each vector space $V$. In other words, let's choose a linear isomorphism $I_V : V \to k^n$ for each $n$-dimensional vector space $V$. Then we can define $G(L) : k^n \to k^m$ as the composition

$$k^n \xrightarrow{I_V^{-1}} V \xrightarrow{G} U \xrightarrow{I_U} k^m.$$

In more down-to-earth terms, $G(L)$ is a matrix of $L$ in coordinates associated to our choice of bases in $V$ and in $U$. Then it is immediate that $G$ is essentially surjective (in fact just surjective) and it is easy to see that $G$ is fully faithful: linear maps from $V$ to $U$ are identified with linear maps from $k^n$ to $k^m$.

§1.4. **Representable Functors.** Fix an object $X \in C$. A very general and useful idea is to study $X$ by poking it with other objects of $C$ or by poking other objects by $X$. This is formalized as follows:

DEFINITION 1.4.1. A *contravariant* functor represented by $X$ is a functor

$$h_X : C \to \mathbf{Sets}$$

that sends any $Y \in C$ to the set of morphisms $\mathbf{Mor}(Y, X)$ and that sends any morphism $Y_1 \xrightarrow{f} Y_2$ the function $\mathbf{Mor}(Y_2, X) \to \mathbf{Mor}(Y_1, X)$ obtained by taking composition with $f$.

Similarly, a *covariant* functor represented by $X$ is a functor

$$h'_X : C \to \mathbf{Sets}$$

that sends any $Y \in C$ to the set of morphisms from $X$ to $Y$and that sends any morphism $Y_1 \xrightarrow{f} Y_2$ the function $\mathbf{Mor}(X, Y_1) \to \mathbf{Mor}(X, Y_2)$ obtained by taking composition with $f$.

An interesting game is to start with a functor and try to guess if it's represented or not. For example, let's consider a forgetful covariant functor

$$\mathbf{Ab} \to \mathbf{Sets}$$

that sends any Abelian group to the set of its elements. Is it representable? We have to decide if there exists an Abelian group $X$ such that morphisms from $X$ to $Y$ are in bijective correspondence with elements of $Y$. We claim that $X = \mathbb{Z}$ works. Indeed, a morphism from $\mathbb{Z}$ to an Abelian group $Y$ is uniquely determined by the image of $1 \in \mathbb{Z}$. And for any element of $Y$, we can define a homomorphism $\mathbb{Z} \to Y$ that sends 1 to this element! So, quite remarkably, $h_{\mathbb{Z}}$ is nothing but the forgetful functor $\mathbf{Ab} \to \mathbf{Sets}$.

See exercises and Section §2.3 for further discussion and examples.

§1.5. **Products and Coproducts.** In some categories, such as **Sets** or $\mathbf{Vect}_k$, there is a natural notion of a product, for example if $X$ and $Y$ are two sets then $X \times Y$ is their Cartesian product. What could a definition of a product look like in other categories? If objects of our category are sets with some extra structure then we can try to define the product of two objects as their set-theoretic product endowed with this extra structure. For example, the product of two vector spaces $U$ and $V$ as a set is just the Cartesian product. Extra structures here are addition of vectors and multiplication of scalars: those are defined component-wise. But this approach clearly depends on the specific nature of the category at hand. And more importantly, it does not always work even in some very basic examples (such as fibered products of manifolds). Quite remarkably, there is another approach to products that does not use specifics of the category. Instead, it is based on the analysis of what the morphism from (or to) the product should look like. One can use the language of representable functors for this, but it will be easier to give an ad hoc definition.

DEFINITION 1.5.1. Let $X$ and $Y$ be objects of a category $C$. Their product (if it exists) is an object $Z$ of $C$ and two morphisms, $\pi_X : Z \to X$ and $\pi_Y : Z \to Y$ (called projections) such that the following "universal property" is satisfied. If $W$ is another object of $C$ endowed with morphisms $a : W \to X$ and $b : W \to Y$ then there exists a unique morphism $f : W \to Z$ such that $a = \pi_X \circ f$ and $b = \pi_Y \circ f$.

For example, suppose that $X$ and $Y$ are sets. Then we can take the Cartesian product $X \times Y$ as $Z$. The projections are just the usual projections: $\pi_X(x, y) = x$ and $\pi_Y(x, y) = y$. If we have functions $a : W \to X$ and $b : W \to Y$ then there is only one choice for a function $f : W \to X \to Y$, namely $f(w) = (a(w), b(w))$. So $X \times Y$ is indeed a product of $X$ and $Y$ according to the definition above.

A little tinkering with this definition gives coproducts:

DEFINITION 1.5.2. Let $X$ and $Y$ be objects of a category $C$. Their coproduct (if it exists) is an object $Z$ of $C$ and two morphisms, $i_X : X \to Z$ and $\pi_Y : Y \to Z$ such that the following "universal property" is satisfied. If $W$ is another object of $C$ endowed with morphisms $a : X \to W$ and $b : Y \to W$ then there exists a unique morphism $f : Z \to W$ such that $a = f \circ i_X$ and $b = f \circ i_Y$.

EXAMPLE 1.5.3. What is a coproduct of two sets? We claim that it is nothing but their disjoint union $X \sqcup Y$ with two inclusions $i_X : X \to X \sqcup Y$ and $i_Y : Y \to X \sqcup Y$. If we have maps $a : X \to W$ and $b : Y \to W$ then it is easy to define $f : X \sqcup Y \to W$: if $x \in X$ then $f(x) = a(x)$ and if $y \in Y$ then $f(y) = b(y)$.

EXAMPLE 1.5.4. What is a coproduct of two vector spaces, $U$ and $V$? Taking the disjoint union of $U$ and $V$ is not a vector space in any reasonable way, so this is not the right way to go. It is quite remarkable that a coproduct exists, and is in fact equal to the product $U \times V$. The maps $i_U$ and $i_V$ are defined as follows: $i_U(u) = (u, 0)$ and $i_V(v) = (0, v)$. If we have maps $a : U \to W$ and $b : V \to W$ then $f : U \times V \to W$ is defined as follows: $f(u, v) = a(u) + b(v)$. It is quite easy to check that this is indeed a coproduct.

The difference between the product and coproduct of vector spaces becomes more transparent if we try to multiply more than two vector spaces. In fact, the product of any collection $\{V_i\}_{i\in I}$ of vector spaces is simply their Cartesian product (with a component-wise addition) but for a coproduct we have to make some changes, otherwise in the definition of the map $f$ as in the previous Example we would have to allow infinite sums, which is not possible. In fact, the right definition of a coproduct is to take a direct sum $\bigoplus_{i\in I} V_i$. By definition, this is a subset of the direct product $\prod_{i\in I} V_i$ that parametrizes all collections $(v_i)_{i\in I}$ of vectors such that all but finitely many of $v_i$'s are equal to $0$. Then we can define the map $f$ exactly as in the previous Example: if we have maps $a_i : V_i \to W$ for any $i$ then $f : \bigoplus_{i\in I} V_i \to W$ takes $(v_i)_{i\in I}$ to $\sum_i a_i(v_i)$.

§1.6. **Natural Transformations.** As Saunders Maclane famously said: "I did not invent category theory to talk about functors. I invented it to talk about natural transformations." So what is a natural transformation? It is a map form one functor to another! Let me start with an example that explains why we might need such a thing.

Recall that for any vector space $V$, we have a "natural" linear map

$$\alpha_V : V \to V^{**}$$

(in fact an isomorphism if $\dim V < \infty$) that sends a vector $v \in V$ to the linear functional $f \mapsto f(v)$ on $V^*$. How is this map "natural"?

One explanation is that $\alpha_V$ does not depend on any choices. After all, if $\dim V < \infty$ then $V$ and $V^*$ are isomorphic as well but there is no special choice for this isomorphism unless we fix a basis of $V$. But this explanation is still "linguistic", the question is, can we *define* naturality mathematically?

To get to the answer, let's study the effect of $\alpha_V$ on morphisms (this is a general recipe of category theory, look not just at objects but also at morphisms). Let $U \xrightarrow{L} V$ be a linear map. We also have our "natural" linear maps $\alpha_U : U \to U^{**}$ and $\alpha_V : V \to V^{**}$. Finally, by taking a contragredient linear map twice, we have a contragredient linear map $U^{**} \xrightarrow{L^{**}} V^{**}$. To summarize things, we have a square of linear maps:

$$\begin{array}{ccc} U & \xrightarrow{\alpha_U} & U^{**} \\ {\scriptstyle L}\downarrow & & \downarrow{\scriptstyle L^{**}} \\ V & \xrightarrow[\alpha_V]{} & V^{**} \end{array} \tag{1}$$

Apriori, there is no reason for this diagram to be commutative: if $\alpha_U$ were a random linear map, this diagram obviously won't be commutative. However, it is easy to see that this diagram is commutative. Let's show it by chasing the diagram. Pick $u \in U$. Then we claim that

$$\alpha_V(L(u)) = L^{**}(\alpha_U(u)).$$

Both sides of this equation are elements of $V^{**}$, i.e. linear functionals on $V^*$. The functional on the LHS takes $f \in V^*$ to $f(L(u))$. The functional on the

RHS takes $f \in V^*$ to

$$\alpha_U(u)(L^*(f)) = L^*(f)(u) = f(L(u)).$$

This calculation might look confusing, but I don't think there is any way to make it more palatable, my only suggestion is to redo this calculation yourself!

Now let's give a general definition.

DEFINITION 1.6.1. Let $F, G : C_1 \to C_2$ be two covariant functors. A *natural transformation* $\alpha : F \to G$ between them is a rule that, for each object $X \in C_1$, assigns a morphism $F(X) \xrightarrow{\alpha_X} G(X)$ in $C_2$ such that the following condition is satisfied. For any morphism $X_1 \xrightarrow{f} X_2$ in $C_1$, we have a commutative diagram

$$\begin{array}{ccc} F(X_1) & \xrightarrow{\alpha_{X_1}} & G(X_1) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(X_2) & \xrightarrow[\alpha_{X_2}]{} & G(X_2) \end{array} \tag{2}$$

If $\alpha_X$ is an isomorphism for any $X$ then $\alpha$ is called a *natural isomorphism*.

How is this related to the linear algebra example above? Let $\mathbf{Vect}_k$ be the category of vector spaces over $k$. Consider two functors: the identity functor $\mathrm{Id} : \mathbf{Vect}_k \to \mathbf{Vect}_k$ and the "double duality" functor $D : \mathbf{Vect}_k \to \mathbf{Vect}_k$ that sends any vector space $V$ to $V^{**}$ and any linear map $L : U \to V$ to a double contragredient linear map $L^{**} : U^{**} \to V^{**}$.

We claim that there is a natural transformation from $\mathrm{Id}$ to $D$ (and in fact a natural isomorphism if we restrict to a subcategory of finite-dimensinal vector spaces). All we need is a rule $\alpha_V$ for each vector space: it should be a morphism, i.e. a linear map, from $\mathrm{Id}(V) = V$ to $D(V) = V^{**}$ such that (2) is satisfied for any morphism $U \to V$. This is exactly the linear map we have constructed above, and (1) is a commutative square we need.

See exercises and Section §2.3 for further discussion and examples.

## §1.7. **Exercises.**

**1.** Let $C$ be a category. (a) Prove that an identity morphism $A \to A$ is unique for each object $A \in \mathbf{Ob}(C)$. (b) Prove that each isomorphism in $C$ has a unique inverse.

**2.** Let $C$ be a category. An object $X$ of $C$ is called an *initial* object (resp. a *terminal* object) if, for every object $Y$ of $C$, there exists a unique morphism $X \to Y$ (resp. a unique morphism $Y \to X$). (a) Decide if the following categories contain initial objects, and if so, describe them: the category of vector spaces, the category of groups, the category of commutative rings (with 1). (b) Prove that a terminal object (if exists) is unique up to a canonical isomorphism (and what exactly does it mean?).

**3.** Let $(I, \leq)$ be a poset (partially ordered set) and let $C_I$ be the corresponding category. Unwind definitions (i.e. give definitions in terms of the poset, without using any categorical language) of (a) terminal and initial objects in $C_I$ (if they exist); (b) product and coproduct in $C_I$ (if they exist).

**4.** Let $X$ be a fixed object of a category $C$. We define a new category $C/X$ of *objects of $C$ over $X$* as follows: an object of $C/X$ is an object $Y$ of $C$ along with some morphism $Y \to X$. In other words, an object of $C/X$ is an arrow $Y \to X$. A morphism from $Y \to X$ to $Y' \to X$ is a morphism from $Y$ to $Y'$ that makes an obvious triangle commutative. Prove that $C/X$ is indeed a category and that $1_X : X \to X$ is its terminal object.

**5.** In the notation of Problem 3, let $C_I$ be the category associated with a poset $I$ and let $\mathbf{Ab}$ be the category of Abelian groups. A contravariant functor $C_I \to \mathbf{Ab}$ is called an *inverse system* of Abelian groups indexed by a partially ordered set $I$. (a) Reformulate this definition without using categorical language. (b) Consider Abelian groups $\mathbb{Z}/2^n\mathbb{Z}$ for $n = 1, 2, \ldots$ and natural homomorphisms $\mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^m\mathbb{Z}$ for $n \geq m$. Show that this is an inverse system. (c) Let $C$ be an arbitrary category. Give a definition of an inverse system of objects in $C$ indexed by a poset $I$. Show that (b) is an inverse system of rings.

**6.** In the notation of Problem 4, fix some inverse system $F : C_I \to \mathbf{Ab}$. Also, let's fix an Abelian group $A$ and consider an inverse system $F_A : C_I \to \mathbf{Ab}$ defined as follows: $F_A(i) = A$ for any $i \in I$ and if $i \leq j$ then the corresponding morphism $A \to A$ is the identity. (a) Prove that $F_A$ is indeed an inverse system. (b) Show that the rule $A \to F_A$ can be extended to a functor from the category $\mathbf{Ab}$ to the category of inverse systems $C_I \to \mathbf{Ab}$ (with natural transformations as morphisms). (c) Unwind definitions to describe what it means to have a natural transformation from $F_A$ to $F$ without categorical language.

**7.** In the notation of Problem 6, an Abelian group $A$ is called an *inverse limit* of an inverse system $F : C_I \to \mathbf{Ab}$ if for any Abelian group $B$, and for any natural transformation $F_B \to F$, there exists a unique homomorphism $B \to A$ such that $F_B$ factors through $F_A$. (a) Unwind definitions to describe the inverse limit without categorical language. (b) Show that the inverse system of rings in Problem 5(b) has an inverse limit (called the ring of 2-adic numbers).

**8.** Let $F : \mathbf{Sets} \to \mathbf{Sets}$ be a contravariant functor that sends any set $S$ to the set of subsets of $S$ and any function $f : S \to S'$ to a function that sends $U \subset S'$ to $f^{-1}(U) \subset S$. (a) Show that $F$ is representable by a two-element set $\{0, 1\}$. (b) Describe a contravariant functor representable by a three-element set $\{0, 1, 2\}$.

**9.** Let $V$ be a real vector space. Prove that its complexification $V_{\mathbb{C}}$ represents the covariant functor $F : \mathbf{Vect}_{\mathbb{C}} \to \mathbf{Sets}$. Namely, for any complex vector space $U$, $F(U)$ is the set of $\mathbb{R}$-linear maps $V \to U_{\mathbb{R}}$ (where $U_{\mathbb{R}}$ is $U$ considered as a real vector space).

**10.** Let $C$ and $D$ be categories and let $F : C \to D$ and $G : D \to C$ be functors. Then $F$ is called a *left adjoint* of $G$ (and $G$ is called a *right adjoint* of $F$) if, for each pair of objects $X \in C$ and $Y \in D$, there exist bijections of sets

$$\tau_{X,Y} : \mathbf{Mor}_D(F(X), Y) \to \mathbf{Mor}_C(X, G(Y))$$

that are natural transformations in $X$ for fixed $Y$ and in $Y$ for fixed $X$. (a) Explain what this last condition means explicitly. (b) Show that complexification $\mathbf{Vect}_{\mathbb{R}} \to \mathbf{Vect}_{\mathbb{C}}$ and restriction of scalars $\mathbf{Vect}_{\mathbb{C}} \to \mathbf{Vect}_{\mathbb{R}}$ are adjoint functors.

**11.** Let $G: \mathbf{Vect}_k \to \mathbf{Sets}$ be a forgetful functor. Describe its left-adjoint.

**12.** Let $C$ be a category and let $X, Y \in \mathbf{Ob}(C)$. Consider representable functors $C \to \mathbf{Sets}$ given by $X$ and $Y$, i.e. $h_X = \mathbf{Mor}(\cdot, X)$ and $h_Y = \mathbf{Mor}(\cdot, Y)$. Show that there is a natural bijection between morphisms $X \to Y$ and natural transformations $h_X \to h_Y$. More precisely, let $D$ be a category of functors $C \to \mathbf{Sets}$ (with natural transformations as morphisms). Show that the rule $X \to h_X$ extends to a fully-faithful functor $C \to D$.

**13.** Show that equivalence of categories is an equivalence relation on categories, i.e. if $C$ and $D$ are equivalent then $D$ and $C$ are also equivalent, and that if $C$ and $D$ (resp. $D$ and $E$) are equivalent then $C$ and $E$ are also equivalent. This relations is obviously reflexive: any category is equivalent to itself by means of the identity functor $\mathrm{Id}_C: C \to C$.

**14.** Give example of a category where (a) products do not always exist; (b) products exist but coproducts do not always exist.

## §2. Tensor Products

§2.1. **Tensor Product of Vector Spaces.** Let's define tensor products in the category of vector spaces over a field $k$. Fix two vector spaces, $U$ and $V$. We want to understand all bilinear maps

$$U \times V \xrightarrow{\beta} W,$$

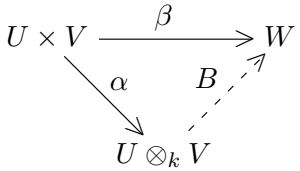
where $W$ can be any vector space. For example, if $W = k$, then $\beta$ is just a bilinear function. We are not going to fix $W$, instead we allow it to vary.

Notice that if $U \times V \to \tilde{W}$ is a bilinear map, and $\tilde{W} \to W$ is a linear map, then the composition $U \times V \to \tilde{W} \to W$ is again bilinear. So we can ask if there exists the "biggest" bilinear map $U \times V \to \tilde{W}$ such that any other bilinear map $U \times V \to W$ factors through some linear map $\tilde{W} \to W$. It turns out that this universal $\tilde{W}$ exists. It is known as a tensor product.

Definition 2.1.1. A vector space $U \otimes_k V$, and a bilinear map

$$U \times V \xrightarrow{\alpha} U \otimes_k V$$

is called a *tensor product* if, for any bilinear map $U \times V \xrightarrow{\beta} W$, there exists a unique linear map $U \otimes_k V \xrightarrow{B} W$ (called a *linear extension* of $\beta$) such that the following diagram commutes:




(3)

Theorem 2.1.2. *The tensor product exists and is unique (up to isomorphism).*

We will prove this theorem later, when we discuss more general tensor products of $R$-modules. But first let's analyze how $U \otimes_k V$ looks like.

DEFINITION 2.1.3. For any pair $(u, v) \in U \times V$, its image $\alpha(u, v) \in U \otimes_k V$ is called a *pure tensor* or an *indecomposable tensor*, and it is denoted by $u \otimes v$.

LEMMA 2.1.4. *$U \otimes_k V$ is spanned by pure tensors (but be careful, not any element of $U \otimes_k V$ is a pure tensor!) We have bilinear relations between pure tensors:*

$$(au_1 + bu_2) \otimes v = a(u_1 \otimes v) + b(u_2 \otimes v), \tag{4}$$

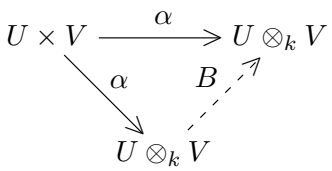
$$u \otimes (av_1 + bv_2) = a(u \otimes v_1) + b(u \otimes v_2). \tag{5}$$

*If $\{e_i\}$ is a basis of $U$ and $\{f_j\}$ is a basis of $V$ then $\{e_i \otimes f_j\}$ is a basis of $U \otimes_k V$. In particular,*

$$\dim(U \otimes_k V) = (\dim U) \cdot (\dim V)$$

*(assuming $U$ and $V$ are finite-dimensional).*

*Proof.* We are going to define various interesting bilinear maps and analyze the universal property (3). For example, let's take a bilinear map $\beta = \alpha$:




Commutativity of the diagram simply means that

$$B(u \otimes v) = \alpha(u, v) = u \otimes v$$

for any pair $(u, v)$. So we see that the restriction of $B$ to the linear span of pure tensors must be the identity map. Suppose that pure tensors don't span the whole $U \otimes_k V$. Then there are many ways to extend a linear map $B$ from the linear span of pure tensors to the whole $U \otimes_k V$. In particular, $B$ is not unique, which contradicts the universal property.

The fact that pure tensors satisfy bilinear relations simply follows from the fact that $\alpha$ is a bilinear map. For example,

$$\alpha(au_1 + bu_2, v) = a\alpha(u_1, v) + b\alpha(u_2, v),$$

which by definition implies

$$(au_1 + bu_2) \otimes v = a(u_1 \otimes v) + b(u_2 \otimes v).$$

It follows from bilinearity that if $u = \sum x_i e_i$ and $v = \sum y_j f_j$ then

$$u \otimes v = \sum x_i y_j (e_i \otimes f_j).$$

Since $U \otimes_k V$ is spanned by pure tensors, we see that in fact $U \otimes_k V$ is spanned by vectors $e_i \otimes f_j$. To show that these vectors form a basis, it remains to show that they are linearly independent.

Suppose that some linear combination is trivial:

$$\sum a_{ij} e_i \otimes f_j = 0. \tag{6}$$

How to show that each $a_{ij} = 0$? Let's fix two indices, $i_0$ and $j_0$, and consider a bilinear function $U \times V \xrightarrow{\beta} k$ defined as follows:

$$\beta\left(\sum x_i e_i, \sum y_j f_j\right) = x_{i_0} y_{j_0}.$$

Then $\beta(e_{i_0}, f_{j_0}) = 1$ and $\beta(e_i, f_j) = 0$ for any other pair of basis vectors. Now we compute its linear extension applied to our linear combination:

$$B\left(\sum a_{ij} e_i \otimes f_j\right) = \sum a_{ij} B(e_i \otimes f_j) = a_{i_0 j_0}.$$

On the other hand,

$$B\left(\sum a_{ij} e_i \otimes f_j\right) = B(0) = 0.$$

So all coefficients $a_{ij}$ in (6) must vanish. □

§2.2. **Tensor Product of $R$-modules.** We will extend the notion of tensor products to the category $\mathbf{Mod}_R$ of $R$-modules, where $R$ is a commutative ring with 1. To stress analogy with vector spaces, instead of saying "homomorphism of $R$-modules", we will say "$R$-linear map of $R$-modules". We fix two $R$-modules, $M$ and $N$ and study $R$-bilinear maps $M \times N \to K$, where $K$ is an arbitrary $R$-module. The definition and the main theorem are the same:

DEFINITION 2.2.1. An $R$-module $M \otimes_R N$ endowed with an $R$-bilinear map

$$M \times N \xrightarrow{\alpha} M \otimes_R N$$

is called a *tensor product* if, for any $R$-bilinear map $M \times N \xrightarrow{\beta} K$, there exists a unique $R$-linear map $M \otimes_R N \xrightarrow{B} K$ (called a *linear extension* of $\beta$) such that the following diagram commutes:

$$\begin{array}{ccc} M \times N & \xrightarrow{\quad\beta\quad} & K \\ & \searrow^{\alpha} \quad \nearrow_{B} & \\ & M \otimes_R N & \end{array} \tag{7}$$

THEOREM 2.2.2. *The tensor product exists.*

*Proof.* We are just going to define $M \otimes_R N$ as an $R$-module generated by pure tensors $u \otimes v$ modulo bilinear relations (4) and (5). But to avoid notational chaos, let's proceed a bit more formally. Let $W$ be a free $R$-module with one basis vector $[m, n]$ for each pair of elements $m \in M$, $n \in N$. There are many pairs, so this is a really huge $R$-odule! Let $W_0 \subset W$ be a submodule spanned by all expressions

$$[au_1 + bu_2, v] - a[u_1, v] - b[u_2, v]$$

and

$$[u, av_1 + bv_2] - a[u, v_1] - b[u, v_2].$$

We define

$$M \otimes_R N := W/W_0$$

(quotient $R$-module). We define pure tensors $u \otimes v$ as cosets of $[u, v]$:

$$u \otimes v := [u, v] + W_0.$$

Then we have

$$(au_1 + bu_2) \otimes v = a(u_1 \otimes v) + b(u_2 \otimes v)$$

and

$$u \otimes (av_1 + bv_2) = a(u \otimes v_1) + b(u \otimes v_2).$$

We define a map

$$M \times N \xrightarrow{\alpha} M \otimes_R N, \quad \alpha(u, v) = u \otimes v.$$

Equations above show that $\alpha$ is bilinear.

Why does $\alpha$ satisfy the universal property (7)? Given a bilinear map $M \times N \xrightarrow{\beta} K$, we can define an $R$-linear map $W \xrightarrow{f} K$ by a simple rule

$$f([u, v]) = \beta(u, v)$$

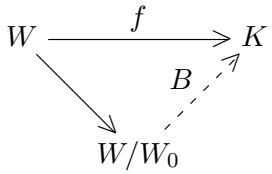
(notice that an $R$-linear map from a free $R$-module can be defined, and is uniquely determined, by its values on the basis). We claim that $W_0 \subset \operatorname{Ker} f$. It is enough to check that $f$ kills generators of $f$. And indeed, we have

$$f\big([au_1+bu_2, v]-a[u_1, v]-b[u_2, v]\big) = \beta(au_1+bu_2, v)-a\beta(u_1, v)-\beta(u_2, v) = 0$$

and

$$f\big([u, av_1+bv_2]-a[u, v_1]-b[u, v_2]\big) = \beta(u, av_1+bv_2)-a\beta(u, v_1)-b\beta(u, v_2) = 0$$

by bilinearity of $\beta$. It follows that $f$ defines an $R$-linear map $W/W_0 \xrightarrow{B} K$:




This map is our bilinear extension $B : M \otimes_R N \to K$.

Finally, notice that we have no choice but to define

$$B(u \otimes v) = \beta(u, v)$$

if we want the diagram (7) to be commutative. So $B$ is unique and $M \otimes_R N$ indeed satisfies the universal property of the tensor product. □

We can generalize Lemma 2.1.4:

LEMMA 2.2.3. *$M \otimes_R N$ is spanned by pure tensors. If $M$ is a free $R$-module with basis $\{e_i\}$ and $N$ is a free $R$-module with basis $\{f_j\}$ then $M \otimes N$ is a free $R$-module with basis $\{e_i \otimes f_j\}$.*

*Proof.* The proof is identical to the proof of Lemma 2.1.4. □

EXAMPLE 2.2.4. Tensor products of non-free $R$-modules are much more interesting. For example, suppose that $R = \mathbb{Z}$, i.e. we are computing tensor products of Abelian groups. What is $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3$? Consider a pure tensor $a \otimes b \in \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3$. Since $a = 3a$ in $\mathbb{Z}_2$, we have

$$a \otimes b = (3a) \otimes b = 3(a \otimes b) = a \otimes (3b) = a \otimes 0 = 0.$$

Since $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3$ is spanned by pure tensors, we have

$$\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 = 0.$$

Next we discuss uniqueness of tensor products.

THEOREM 2.2.5. *Tensor product $M \otimes_R N$ is unique up to a canonical isomorphism.*

*Proof.* Suppose that we have two $R$-modules, let's call them $M \otimes_R N$ and $M \otimes'_R N$, and two bilinear maps, $M \times N \xrightarrow{\alpha} M \otimes_R N$ and $M \times N \xrightarrow{\alpha'} M \otimes'_R N$ that both of them satisfy the universal property. From the diagram

$$\begin{array}{ccc} M \times N & \xrightarrow{\alpha'} & M \otimes'_R N \\ & \searrow^{\alpha} & \\ & & M \otimes_R N \end{array} \tag{8}$$

we deduce existence of unique linear maps

$$M \otimes_R N \xrightarrow{B} M \otimes'_R N \quad \text{and} \quad M \otimes'_R N \xrightarrow{B'} M \otimes_R N$$

that make (8) commutative. We claim that $B$ is an isomorphism and $B'$ is its inverse. Indeed, $B' \circ B$ makes the following diagram commutative:

$$\begin{array}{ccc} M \times N & \xrightarrow{\alpha} & M \otimes_R N \\ & \searrow^{\alpha} \quad \nearrow_{B' \circ B} & \\ & M \otimes_R N & \end{array}$$

But the identity map on $M \otimes_R N$ also makes it commutative. By uniqueness of the linear extension, we see that $B' \circ B = \mathrm{Id}\,|_{M \otimes_R N}$. A similar argument shows that $B \circ B' = \mathrm{Id}\,|_{M \otimes'_R N}$. □

This argument shows that if we have two $R$-modules that satisfy the universal property of the tensor product, then they are not only isomorphic, but in fact there is a canonical *choice* for this isomorphism (given by maps $B$ and $B'$ of the proof). That's why we say that the tensor product $M \otimes_R N$ is unique up to a *canonical* isomorphism. The argument used in the proof above is very general. It can be easily generalized if we recast it in the categorical language. This is done in the next section.

## §2.3. **Categorical aspects of tensors: Yoneda's Lemma.**

DEFINITION 2.3.1. Fix $R$-modules $M$ and $N$ and define a covariant functor

$$\mathit{BilMaps}_{M,N} : \mathbf{Mod}_R \to \mathbf{Sets}$$

that sends any $R$-module $K$ to the set of bilinear maps

$$\{\beta \,|\, M \times N \xrightarrow{\beta} K\}$$

and that sends any $R$-linear map $K \xrightarrow{f} K'$ to the function

$$\{\beta \,|\, M \times N \xrightarrow{\beta} K\} \to \{\beta' \,|\, M \times N \xrightarrow{\beta'} K'\}$$

that assigns to a bilinear function $M \times N \xrightarrow{\beta} K$ with values in $K$ a bilinear function $M \times N \xrightarrow{\beta} K \xrightarrow{f} K'$ with values in $K'$.

The $R$-module $M \otimes_R N$, as any other $R$-module, defines a covariant *representable functor*

$$h_{M\otimes_R N} : \mathbf{Mod}_R \to \mathbf{Sets}$$

that sends an $R$-module $K$ to the set of $R$-linear maps

$$\{B \mid M \otimes_R N \xrightarrow{B} K\}$$

and that sends an $R$-linear map $K \xrightarrow{f} K'$ to the function

$$\{B \mid M \otimes_R N \xrightarrow{B} K\} \to \{B' \mid M \otimes_R N \xrightarrow{B'} K'\}$$

that assigns to an $R$-linear function $M \otimes_R N \xrightarrow{B} K$ with values in $K$ an $R$-function $M \otimes_R N \xrightarrow{B} K \xrightarrow{f} K'$ with values in $K'$.

Now of course the whole point of introducing the tensor product is to identify the set of bilinear maps $M \times N \to K$ with the set of linear maps $M \otimes_R N \to K$. How exactly is this done? Recall that we also have a "universal" bilinear map

$$M \times N \xrightarrow{\alpha} M \otimes_R N.$$

For any linear map $M \otimes_R N \xrightarrow{B} K$, $B \circ \alpha$ is a bilinear map $M \times N \longrightarrow K$. And vice versa, for any bilinear map $M \times N \xrightarrow{\beta} K$, there exists a unique linear map $M \otimes_R N \xrightarrow{B} K$ such that $B \circ \alpha = \beta$.

In other words, for any $R$-module $K$, we have a bijection of sets

$$h_{M\otimes_R N}(K) \xrightarrow{\alpha_K} \mathit{BilMaps}_{M,N}(K)$$

where $\alpha_K$ simply composes a linear map $M \otimes_R N \to K$ with $\alpha$.

LEMMA 2.3.2. *This gives a natural isomorphism of functors*

$$\alpha : h_{M\otimes_R N} \to \mathit{BilMaps}_{M,N}.$$

*Proof.* Natural transformations and natural isomorphisms are defined in Section §1.6. We need a rule that for each $R$-module $K$ gives a bijection $\alpha_K$ of sets (recall that isomorphisms in the category of sets are called bijections)

$$h_{M\otimes_R N}(K) \to \mathit{BilMaps}_{M,N}(K)$$

from the set of linear maps $M \otimes_R N \to K$ to the set of bilinear maps $M \times N \to K$. We have already defined this bijection, this is just a bijection given by taking composition with a universal bilinear map $M \times N \to M \otimes_R N$.

It remains to check that the square (2) is commutative. Take an $R$-linear map $K_1 \xrightarrow{f} K_2$. We have to check that the following square is commutative:

$$\begin{array}{ccc} h_{M\otimes_R N}(K_1) & \xrightarrow{\alpha_{K_1}} & \mathit{BilMaps}_{M,N}(K_1) \\ \Big\downarrow{\scriptstyle h_{M\otimes_R N}(f)} & & \Big\downarrow{\scriptstyle \mathit{BilMaps}_{M,N}(f)} \\ h_{M\otimes_R N}(K_2) & \xrightarrow[\alpha_{K_2}]{} & \mathit{BilMaps}_{M,N}(K_2) \end{array}$$

Let's chase the diagram. Take an element of $h_{M\otimes_R N}(K_1)$, i.e. an $R$-linear map

$$M \otimes_R N \xrightarrow{B} K_1.$$

The horizontal arrow $\alpha_{K_1}$ takes it to the bilinear map

$$M \times N \xrightarrow{\alpha} M \otimes_R N \xrightarrow{B} K_1$$

and then the vertical map $\mathit{BilMaps}_{M,N}(f)$ takes it to the bilinear map

$$M \times N \xrightarrow{\alpha} M \otimes_R N \xrightarrow{B} K_1 \xrightarrow{f} K_2.$$

On the other hand, if we apply the vertical arrow $h_{M\otimes_R N}(f)$ first, we will get a linear map

$$M \otimes_R N \xrightarrow{B} K_1 \xrightarrow{f} K_2$$

and applying $\alpha_{K_2}$ gives a bilinear map

$$M \times N \xrightarrow{\alpha} M \otimes_R N \xrightarrow{B} K_1 \xrightarrow{f} K_2,$$

the same as above. So the square commutes. □

If we can define a tensor product of $M$ and $N$ in two different ways, say $M \otimes_R N$ and $M \otimes'_R N$, the representable functors $h_{M\otimes_R N}$ and $h_{M\otimes'_R N}$ are going to be naturally isomorphic (because both of them are naturally isomorphic to $\mathit{BilMaps}_{M,N}$). So to reprove Theorem 2.2.5, we can use the following weak version of Yoneda's lemma:

LEMMA 2.3.3. *Let $X, Y$ be two objects in a category $C$. Suppose we have a natural isomorphism of representable functors $\alpha : h_X \to h_Y$. Then $X$ and $Y$ are canonically isomorphic.*

*Proof.* To match our discussion of the tensor product, we will prove a covariant version, the contravariant version has a similar proof. Recall that $h_X$ sends any object $Z$ to the set $\mathbf{Mor}(X, Z)$ and it sends any morphism $Z_1 \to Z_2$ to the function $\mathbf{Mor}(X, Z_1) \to \mathbf{Mor}(X, Z_2)$ obtained by taking a composition with $Z_1 \to Z_2$.

So $\alpha$ gives, for any object $Z$ in $C$, a bijection

$$\alpha_Z : \mathbf{Mor}(X, Z) \to \mathbf{Mor}(Y, Z)$$

such that for each morphism $Z_1 \to Z_2$ we have a commutative diagram

$$\begin{array}{ccc} \mathbf{Mor}(X, Z_1) & \xrightarrow{\alpha_{Z_1}} & \mathbf{Mor}(Y, Z_1) \\ \downarrow & & \downarrow \\ \mathbf{Mor}(X, Z_2) & \xrightarrow[\alpha_{Z_2}]{} & \mathbf{Mor}(Y, Z_2) \end{array}$$

where the vertical arrows are obtained by composing with $Z_1 \to Z_2$.

In particular, we have bijections

$$\mathbf{Mor}(X, X) \xrightarrow{\alpha_X} \mathbf{Mor}(Y, X) \quad \text{and} \quad \mathbf{Mor}(X, Y) \xrightarrow{\alpha_Y} \mathbf{Mor}(Y, Y).$$

We define morphisms

$$f = \alpha_X(\mathrm{Id}_X) \in \mathbf{Mor}(Y, X) \quad \text{and} \quad g = \alpha_Y^{-1}(\mathrm{Id}_Y) \in \mathbf{Mor}(X, Y).$$

We claim that $f$ and $g$ are inverses of each other, and in particular $X$ and $Y$ are canonically isomorphic (by $f$ and $g$). Indeed, consider the commutative square above when $Z_1 = X$, $Z_2 = Y$, and the morphism from $X$ to $Y$ is $g$. It gives

$$\begin{array}{ccc} \mathbf{Mor}(X,X) & \xrightarrow{\alpha_X} & \mathbf{Mor}(Y,X) \\ {\scriptstyle g\circ\cdot}\downarrow & & \downarrow{\scriptstyle g\circ\cdot} \\ \mathbf{Mor}(X,Y) & \xrightarrow[\alpha_Y]{} & \mathbf{Mor}(Y,Y) \end{array}$$

Let's take $\mathrm{Id}_X \in \mathbf{Mor}(X,X)$ and compute its image in $\mathbf{Mor}(Y,Y)$ in two different ways. If we go horizontally, we first get $\alpha_X(\mathrm{Id}_X) = f \in \mathbf{Mor}(Y,X)$. Then we take its composition with $X \xrightarrow{g} Y$ to get $g \circ f \in \mathbf{Mor}(Y,Y)$. If we go vertically first, we get $g \in \mathbf{Mor}(X,Y)$. Then we get $\alpha_Y(g) = \mathrm{Id}_Y$, because $g = \alpha_Y^{-1}(\mathrm{Id}_Y)$. So we see that $g \circ f = \mathrm{Id}_Y$. Similarly, one can show that $f \circ g = \mathrm{Id}_X$, i.e. $f$ and $g$ are really inverses of each other. □

The full (covariant) version of the Yoneda's lemma is this:

LEMMA 2.3.4. *Let $C$ be a category. For any object $X$ of $C$, consider a covariant representable functor $h_X : C \to \mathbf{Sets}$. For any morphism $X_1 \xrightarrow{f} X_2$, consider a natural transformation $h_{X_2} \to h_{X_1}$ defined as follows: for any object $Y$ of $C$, the function*

$$\alpha_Y : h_{X_2}(Y) = \mathbf{Mor}(X_2,Y) \xrightarrow{\cdot\circ f} \mathbf{Mor}(X_1,Y) = h_{X_1}(Y)$$

*is just a composition of $g \in \mathbf{Mor}(X_2,Y)$ with $X_1 \xrightarrow{f} X_2$. This gives a functor from $C$ to the category of covariant functors $C \to \mathbf{Sets}$ (with natural transformations as morphisms).*

*This functor is fully faithful, i.e. the set of morphisms $X_1 \to X_2$ in $C$ is identified with the set of natural transformations $h_{X_2} \to h_{X_1}$.*

*Proof.* For any morphism $X_1 \xrightarrow{f} X_2$, the natural transformation $\alpha : h_{X_2} \to h_{X_1}$ is defined in the statement of the Lemma. Now suppose we are given a natural transformation $\alpha : h_{X_2} \to h_{X_1}$. Applying $\alpha_{X_2}$ to $\mathrm{Id}_{X_2} \in \mathbf{Mor}(X_2,X_2)$ gives some morphism $f \in \mathbf{Mor}(X_1,X_2)$. We claim that this establishes a bijection between $\mathbf{Mor}(X_1,X_2)$ and natural transformations $h_{X_2} \to h_{X_1}$.

Start with $f \in \mathbf{Mor}(X_1,X_2)$. Then $\alpha_{X_2} : \mathbf{Mor}(X_2,X_2) \to \mathbf{Mor}(X_1,X_2)$ is obtained by composing with $f$. In particular, $\alpha_{X_2}(\mathrm{Id}_{X_2}) = f$.

Finally, let us start with a natural transformation $\alpha : h_{X_2} \to h_{X_1}$. Then

$$f = \alpha_{X_2}(\mathrm{Id}_{X_2}) \in \mathbf{Mor}(X_1,X_2).$$

It defines a natural transformation $\beta : h_{X_2} \to h_{X_1}$. We have to show that $\alpha = \beta$, i.e. that for any $Y \in C$, the map $\alpha_Y : \mathbf{Mor}(X_2,Y) \to \mathbf{Mor}(X_1,Y)$ is just a composition with $f$. The argument is the same as in the previous Lemma. Start with any $g \in \mathbf{Mor}(X_2,Y)$ and consider a commutative

square

$$\begin{array}{ccc} \mathbf{Mor}(X_2, X_2) & \xrightarrow{\alpha_{X_2}} & \mathbf{Mor}(X_1, X_2) \\ \downarrow & & \downarrow \\ \mathbf{Mor}(X_2, Y) & \xrightarrow[\alpha_Y]{} & \mathbf{Mor}(X_1, Y) \end{array}$$

where the vertical maps are compositions with $X_2 \xrightarrow{g} Y$. Take $\mathrm{Id}_{X_2}$ and follow it along the diagram. We get

$$\begin{array}{ccc} \mathrm{Id}_{X_2} & \xrightarrow{\alpha_{X_2}} & f \\ \downarrow & & \downarrow \\ g & \xrightarrow[\alpha_Y]{} & \alpha_Y(g) = g \circ f \end{array}$$

So $\alpha_Y(g)$ is exactly what we want: simply a composition with $f$. □

Why is Yoneda's lemma useful? Very often we have to deal with situations when it is hard to construct a morphism $X \to Y$ between two objects in the category directly. For example, it is hard to construct an explicit differentiable map from one manifold to another. Yoneda's lemma gives an indirect way of constructing morphisms. Of course, it works only if we have a good understanding of (covariant or contravariant) functors $h_X$ and $h_Y$. In this case we can try to define a natural transformation between these functors instead of defining the morphism $X \to Y$ directly. Let's work out a simple example of this.

LEMMA 2.3.5. *For any $R$-modules $M$ and $N$, we have a canonical isomorphism*

$$M \otimes_R N \simeq N \otimes_R M.$$

*Proof.* Of course this isomorphism just takes a pure tensor $m \otimes n$ to $n \otimes m$. But since pure tensors are linearly dependent, we have to check that this morphism is well-defined. For example, we can look at a bilinear map $M \times N \to N \otimes_R M$ that sends $(m, n) \to n \otimes m$ and use the universal property to factor this bilinear map through the tensor product $M \otimes_R N$.

Let's repackage this argument to highlight how Yoneda's lemma works. We already know that $h_{M \otimes_R N}$ is naturally isomorphic to the functor of bilinear maps $\mathit{BilMaps}_{M,N}$ and of course $h_{N \otimes_R M}$ is naturally isomorphic to the functor $\mathit{BilMaps}_{N,M}$. So, by Yoneda's lemma, to construct an explicit isomorphism between $M \otimes_R N$ and $N \otimes_R M$ it suffices to construct an explicit natural isomorphism between functors $\mathit{BilMaps}_{M,N}$ and $\mathit{BilMaps}_{N,M}$. In other words, for each $R$-module $K$, we need a bijection $\alpha_K$ between $\mathit{BilMaps}_{M,N}(K)$ and $\mathit{BilMaps}_{N,M}(K)$, i.e. between the set of bilinear maps $M \times N \to K$ and the set of bilinear maps $N \times M \to K$ that behaves "naturally" in $K$, i.e. for each $R$-linear map $K_1 \to K_2$, the following diagram

commutes

$$\begin{array}{ccc} \mathit{BilMaps}_{M,N}(K_1) & \xrightarrow{\alpha_{K_1}} & \mathit{BilMaps}_{N,M}(K_1) \\ \downarrow & & \downarrow \\ \mathit{BilMaps}_{M,N}(K_2) & \xrightarrow{\alpha_{K_2}} & \mathit{BilMaps}_{N,M}(K_2) \end{array}$$

where the vertical maps are just compositions with $K_1 \to K_2$. It is clear that $\alpha_K$ is a very simple transformation: it just takes a bilinear map $M \times N \xrightarrow{\beta} K$ to a bilinear map

$$N \times M \to M \times N \xrightarrow{\beta} K,$$

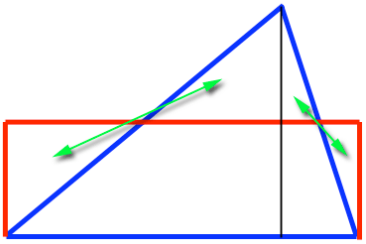
where the first map is a switch $(n, m) \to (m, n)$. □

§2.4. **Hilbert's 3d Problem.** As a fun application of tensors, let's solve the Hilbert's 3d problem:

PROBLEM 2.4.1. *Given two polytopes $P, Q \subset \mathbb{R}^3$ of the same volume, is it always possible to cut $P$ into polyhedral pieces and then reassemble them into $Q$?*

Here a polytope is a 3-dimensional analogue of a polygon: we can define it, for example, as a convex hull of finitely many points in $\mathbb{R}^3$.

For polygons, i.e. in dimension 2, the problem above has a positive solution, which can be seen by applying induction and various simple cutting tricks. For example, it is easy to cut a triangle and then rearrange pieces to get a rectangle: Notice that this actually *proves* that the area of a triangle is



equal to $ah/2$, where $a$ is the base and $h$ is the height.

This is a source of many cute puzzles, for example Figure 1 shows how to cut a square into pieces that can be rearranged to get a regular hexagon.

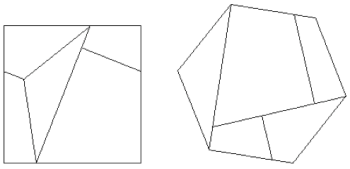


FIGURE 1. Cut and Paste

If the answer to the 3-dimensional Problem were positive, it would be possible to derive volume formulas for polytopes using geometry only.

However, it was known since Archimedes that to prove the volume formula even for a tetrahedron, one has to integrate! So people have long suspected (at least since Gauss) that the answer to the Problem is negative.

After Hilbert stated his famous problems, the third problem was almost immediately solved by his student, Max Dehn. Dehn's idea was to introduce some sort of a hidden volume: some invariant of polytopes different from volume that nevertheless behaves additively if you cut a polytope into pieces. To be more specific, let

$$\Gamma = \mathbb{R} \otimes_{\mathbb{Z}} (\mathbb{R}/\pi\mathbb{Z})$$

(the tensor product of Abelian groups).

DEFINITION 2.4.2. For a polytope $P$, let $E_1, \dots, E_r$ be the collection of its edges. For each edge $E_i$, let $l_i$ be its length and let $\alpha_i$ be the angle between faces meeting along $E_i$. We define the *Dehn invariant* $D(P) \in \Gamma$ as follows:

$$D(P) := \sum_{i=1}^{r} l_i \otimes \alpha_i.$$

EXAMPLE 2.4.3. Let $P$ be a cube with side $a$. The cube has 12 edges, each has length $a$ and angle $\frac{\pi}{2}$. So we have

$$D(P) = \sum_{i=1}^{12} a \otimes \frac{\pi}{2} = a \otimes \left(12\frac{\pi}{2}\right) = a \otimes (6\pi) = a \otimes 0 = 0.$$

We will prove two lemmas:

LEMMA 2.4.4. *If $P$ is cut into polyhedral pieces $P_1, \dots, P_s$ then*

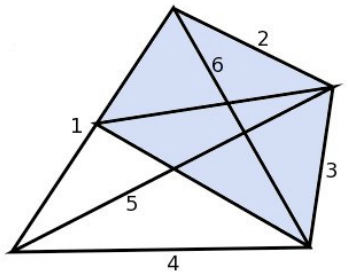
$$D(P) = D(P_1) + \ldots + D(P_s).$$

LEMMA 2.4.5. *If $Q$ is a regular tetrahedron then $D(Q) \neq 0$.*

COROLLARY 2.4.6. *The Hilbert's third problem has a negative solution.*

Indeed, if $P$ is a cube then Lemma 2.4.3 shows that $D(P) = 0$. If $P$ is cut into polyhedral pieces $P_1, \dots, P_s$ then $D(P_1) + \ldots + D(P_s) = 0$ by Lemma 2.4.4. If $Q$ is a regular tetrahedron then $D(Q) \neq 0$ by Lemma 2.4.5. So by Lemma 2.4.4, we can not rearrange pieces $P_1, \dots, P_s$ to get $Q$.

*Proof of Lemma 2.4.4.* A complete proof is a bit tedious, so we will just give a proof "by example" that completely explains what's going on.



Let $P$ be a tetrahedron cut into two tetrahedra, a blue $P'$ and a white $P''$. The polytope $P$ has six edges of length $l_1, \dots, l_6$ and with angles $\alpha_1, \dots, \alpha_6$:

$$D(P) = \sum_{i=1}^{6} l_i \otimes \alpha_i.$$

The first edge of $P$ is cut between $P'$ and $P''$, let $l_1'$ and $l_1''$ be the legths of the corresponding edges. Notice that $l_1 = l_1' + l_1''$. Likewise, the third angle $\alpha_3$ is the sum of angles $\alpha_3'$ and $\alpha_3''$. Also, $P'$ and $P''$ share two new edges, of lengths $m_1$ and $m_2$ and with angles $\beta_1'$, $\beta_1''$, $\beta_2'$ and $\beta_2''$. Notice that $\beta_1' + \beta_1'' = \pi$ and $\beta_2' + \beta_2'' = \pi$. Now we are ready for bookkeeping:

$$D(P') = l_1' \otimes \alpha_1 + l_2 \otimes \alpha_2 + l_3 \otimes \alpha_3' + l_6 \otimes \alpha_6 + m_1 \otimes \beta_1' + m_2 \otimes \beta_2'$$

$$D(P'') = l_1'' \otimes \alpha_1 + l_4 \otimes \alpha_4 + l_3 \otimes \alpha_3'' + l_5 \otimes \alpha_5 + m_1 \otimes \beta_1'' + m_2 \otimes \beta_2''$$

Adding $D(P')$ and $D(P'')$ together, we get

$$(l_1' + l_1'') \otimes \alpha_1 + l_2 \otimes \alpha_2 + l_3 \otimes (\alpha_3' + \alpha_3'') + l_4 \otimes \alpha_4 + l_5 \otimes \alpha_5 + l_6 \otimes \alpha_6 +$$

$$m_1 \otimes (\beta_1' + \beta_1'') + m_2 \otimes (\beta_2' + \beta_2'') =$$

$$l_1 \otimes \alpha_1 + l_2 \otimes \alpha_2 + l_3 \otimes \alpha_3 + l_4 \otimes \alpha_4 + l_5 \otimes \alpha_5 + l_6 \otimes \alpha_6 + m_1 \otimes \pi + m_2 \otimes \pi =$$

$$l_1 \otimes \alpha_1 + l_2 \otimes \alpha_2 + l_3 \otimes \alpha_3 + l_4 \otimes \alpha_4 + l_5 \otimes \alpha_5 + l_6 \otimes \alpha_6 = D(P).$$

We see that Lemma basically follows from the bilinearity of the tensor product and from the fact that each time cutting creates new edges, the sum of angles at these edges adds up to a multiple of $\pi$. □

*Proof of Lemma 2.4.5.* Let $Q$ be a regular hexagon wigth side $a$. By the Law of Cosines, the angle between its faces is equal to $\arccos \frac{1}{3}$. So we have

$$D(Q) = \sum_{i=1}^{6} a \otimes \arccos \frac{1}{3} = (6a) \otimes \arccos \frac{1}{3}.$$

CLAIM 2.4.7. *$a \otimes \alpha = 0$ in $\mathbb{R} \otimes (\mathbb{R}/\pi\mathbb{Z})$ if and only if either $a = 0$ or $\alpha \in \mathbb{Q}\pi$.*

*Proof.* We certainly have $0 \otimes \alpha = 0$. If $\alpha = \frac{m}{n}\pi$ then

$$a \otimes \alpha = a \otimes \frac{m}{n}\pi = \left(n\frac{a}{n}\right) \otimes \left(\frac{m}{n}\pi\right) = \frac{a}{n} \otimes \left(n\frac{m}{n}\pi\right) = \frac{a}{n} \otimes (m\pi) = 0.$$

Now we prove another implication. Fix $a_0 \neq 0$ and $\alpha_0 \neq \frac{m}{n}\pi$. Consider $\mathbb{R}$ as a $\mathbb{Q}$-vector space. Then $a_0$ spans a 1-dimensional subspace $L = \mathbb{Q}a_0$. We have a $\mathbb{Q}$-linear function $L \to \mathbb{Q}$ that sends $a_0$ to 1. This function can be extended to $\mathbb{Q}$-linear function $l : \mathbb{R} \to \mathbb{Q}$ that sends $a_0$ to 1.

We have a $\mathbb{Z}$-bilinear function

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad (a, \alpha) \mapsto l(a)\alpha.$$

$\mathbb{R}$ contains $\pi\mathbb{Q}$ as a $\mathbb{Z}$-submodule. Composing a map above with the projection $\mathbb{R} \to \mathbb{R}/(\pi\mathbb{Q})$, we get a $\mathbb{Z}$-bilinear function

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R}/(\pi\mathbb{Q}), \quad (a, \alpha) \mapsto l(a)\alpha + \pi\mathbb{Q}.$$

Notice that any pair of the form $(a, \pi n)$ is mapped to 0 (because $l(a)$ is a rational number), so our function induces a $\mathbb{Z}$-bilinear function

$$\mathbb{R} \times (\mathbb{R}/\pi\mathbb{Z}) \xrightarrow{\beta} \mathbb{R}/(\pi\mathbb{Q}), \quad (a, \alpha) \mapsto l(a)\alpha + \pi\mathbb{Q}.$$

By the universal property of the tensor product, this bilinear map factors through the tensor product:

$$\begin{array}{ccc} \mathbb{R}\times(\mathbb{R}/\pi\mathbb{Z}) & \xrightarrow{\quad\beta\quad} & \mathbb{R}/(\pi\mathbb{Q}) \\ & \searrow \quad \nearrow & \\ & \mathbb{R}\otimes_{\mathbb{Z}}(\mathbb{R}/\pi\mathbb{Z}) & \end{array}$$

We have

$$\beta(a_0,\alpha_0) = l(a_0)\alpha_0 + \pi\mathbb{Q} = \alpha_0 + \pi\mathbb{Q} \neq 0.$$

Therefore,

$$a_0\otimes\alpha_0 \neq 0.$$

This shows the first Claim. □

CLAIM 2.4.8. *If* $\cos\frac{2\pi m}{n}\in\mathbb{Q}$ *then it is equal to* $1$, $\frac{1}{2}$, $0$, $-\frac{1}{2}$, *or* $-1$. *In particular,*

$$\arccos\frac{1}{3}\notin\mathbb{Q}\pi.$$

*Proof.* Suppose $\cos\frac{2\pi m}{n}\in\mathbb{Q}$. We can assume that $m$ and $n$ are coprime. Let

$$\xi = \cos\frac{2\pi m}{n} + i\sin\frac{2\pi m}{n}\in\mathbb{C}.$$

Then $\xi$ is a primitive $n$-th root of $1$. Let $\mathbb{Q}(\xi)$ be the minimal field containing $\xi$ (a cyclotomic field) and let $[\mathbb{Q}(\xi):\mathbb{Q}]$ be the degree of this field extension, i.e. the dimension of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$. Then

$$\mathbb{Q}(\xi)\subset\mathbb{Q}\left(i\sin\frac{2\pi m}{n}\right) = \mathbb{Q}\left(\sqrt{\cos^2\frac{2\pi m}{n}-1}\right) = \mathbb{Q}(\sqrt{r}),$$

where $r$ is a rational number. So $\mathbb{Q}(\xi)$ is at most a quadratic extension of $\mathbb{Q}$, and therefore,

$$[\mathbb{Q}(\xi):\mathbb{Q}] = 1 \text{ or } 2.$$

On the other hand, a basic fact from the Galois theory that we are going to take on faith here is that

$$[\mathbb{Q}(\xi):\mathbb{Q}] = \phi(n),$$

where an Euler function $\phi(n)$ counts how many numbers between $0$ and $n$ are coprime to $n$, i.e. how many elements of the ring $\mathbb{Z}/n\mathbb{Z}$ are invertible. Take a prime decomposition

$$n = p_1^{k_1}\dots p_s^{k_s}.$$

By the Chinese theorem on remainders, we have an isomorphism of rings

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{k_1}\oplus\ldots\oplus\mathbb{Z}/p_s^{k_s}.$$

This isomorphism induces an isomorphism of groups of invertible elements

$$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1^{k_1})^*\times\ldots\times(\mathbb{Z}/p_s^{k_s})^*.$$

This gives a formula

$$\phi(n) = \phi(p_1^{k_1})\dots\phi(p_s^{k_s}).$$

It is clear that $\phi(p^k) = p^k - p^{k-1}$ because a number is coprime to $p^k$ if and only if it is coprime to $p$, and $\mathbb{Z}/p^k\mathbb{Z}$ contains exactly $p^{k-1}$ elements that are divisible by $p$. So we have

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \dots (p_s^{k_s} - p_s^{k_s-1}) =$$
$$= p_1^{k_1-1} \dots p_s^{k_s-1} \times (p_1 - 1) \dots (p_s - 1).$$

If $\phi(n) \leq 2$ then each $p_i \leq 3$ and each $k_i \leq 2$. Going through the list of possibilities, we see that the only solutions are

$$n = 1, 2, 3, 4, 6.$$

This gives the Claim. □

Combining two claims finishes the proof of the Hilbert's 3d problem. □

§2.5. **Right-exactness of a tensor product.** Let's fix an $R$-module $M$ and study the operation of "tensoring with $M$":

$$N \mapsto N \otimes_R M.$$

This gives a map from the category of $R$-modules to itself. Moreover, for any $R$-linear map $N \xrightarrow{f} N'$, we can define an $R$-linear map

$$N \otimes_R M \xrightarrow{f\otimes \mathrm{Id}} N' \otimes_R M, \quad n \otimes m \mapsto f(n) \otimes m.$$

Of course pure tensors are not linearly independent, so we have to check that $f \otimes \mathrm{Id}$ is well-defined. This can be done as follows. We have a map

$$N \times M \to N' \otimes_R M, \quad (n, m) \mapsto f(n) \otimes m,$$

which is clearly bilinear. So, by the universal property of the tensor product, it gives a linear map

$$N \otimes_R M \to N' \otimes_R M,$$

which is exactly our map $f \otimes \mathrm{Id}$.

LEMMA 2.5.1. *"Tensoring with $M$" functor $\cdot \otimes_R M$ is a functor from the category of $R$-modules to itself.*

*Proof.* To show that something is a functor, we have to explain how it acts on objects and morphisms in the category (this is done above), and then check axioms of a functor. There are two axioms: a functor should preserve identity maps and compositions of maps.

This is an example of a calculation that's much easier to do in your head than to read about. Still, let's give a proof just to show how it's done.

If $N \to N$ is an identity map, then $N \otimes_R M \xrightarrow{\mathrm{Id}\otimes \mathrm{Id}} N \otimes_R M$ is also obviously an identity map.

Suppose we have maps $N \xrightarrow{f} N' \xrightarrow{g} N''$. Let's compute the composition

$$N \otimes_R M \xrightarrow{f\otimes \mathrm{Id}} N' \otimes_R M \xrightarrow{g\otimes \mathrm{Id}} N'' \otimes_R M.$$

It takes a pure tensor $n \otimes m$ to the pure tensor $f(n) \otimes m$ and then to the tensor $g(f(n)) \otimes m = (g \circ f)(n) \otimes m$. The map

$$N \otimes_R M \xrightarrow{(g\circ f)\otimes \mathrm{Id}} N'' \otimes_R M$$

has the same effect on pure tensors. Since pure tensors span $N \otimes_R M$, we see that

$$(g \otimes \mathrm{Id}) \circ (f \otimes \mathrm{Id}) = (g \circ f) \otimes \mathrm{Id},$$

which exactly means that tensoring with $M$ preserves composition. □

LEMMA 2.5.2. *There exists a canonical isomorphism $R \otimes_R M \simeq M$, $r \otimes m \mapsto rm$.*

*Proof 1.* For any $R$-module $K$, an $R$-bilinear map $R \times M \xrightarrow{F} K$ defines an $R$-linear map $M \xrightarrow{f} K$ by formula $f(m) = F(1, m)$. And vice versa, an $R$-linear map $M \xrightarrow{f} K$ defines an $R$-bilinear map $R \times M \xrightarrow{F} K$ by formula $F(r, m) = rf(m)$. This gives a natural (in $K$) bijection between bilinear maps $R \times M \to K$ and linear maps $M \to K$. It follows that functors $\mathit{BilMaps}_{R,M}$ and $h_M$ are naturally isomorphic. It follows that functors $h_{R \otimes_R M}$ and $h_M$ are naturally isomorphic. By Yoneda's lemma, it follows that $R \otimes_R M$ and $M$ themselves are isomorphic. To see that this isomorphism has the form $r \otimes m \mapsto rm$, recall that the proof of Yoneda's lemma is constructive: to find an isomorphism we have to apply the natural transformation to the identity morphism. So take $K = M$ and $f = \mathrm{Id}_M$ in the analysis above. Then $F(r, m) = rm$. □

*Proof 2.* Define a bilinear map $R \times M \to M$ by formula $(r, m) \mapsto rm$. By the universal property of the tensor product, it factors through a linear map

$$R \otimes_R M \xrightarrow{B} M, \quad r \otimes m \mapsto rm.$$

This map is clearly surjective (take $r = 1$). Take a tensor $\sum_i r_i \otimes m_i \in \operatorname{Ker} B$. Then $\sum_i r_i m_i = 0$. It follows that

$$\sum_i r_i \otimes m_i = \sum_i r_i(1 \otimes m_i) = \sum_i 1 \otimes (r_i m_i) =$$

$$= 1 \otimes \left( \sum_i r_i m_i \right) = 1 \otimes 0 = 0.$$

So $B$ is also injective. □

Now the main result:

THEOREM 2.5.3. *$\cdot \otimes_R M$ is a right-exact functor, i.e. for any exact sequence*

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0, \tag{9}$$

*the induced sequence*

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

*is also exact.*

*Proof.* To show that $g \otimes \mathrm{Id}$ is surjective, it suffices to show that any pure tensor $n'' \otimes m \in N'' \otimes_R M$ is in the image of $g \otimes \mathrm{Id}$. But $g$ is surjective, so $n'' = g(n)$ for some $n$, and then $n'' \otimes m = g(n) \otimes m$.

Next we show that

$$\mathrm{Im}(f \otimes \mathrm{Id}) \subset \operatorname{Ker}(g \otimes \mathrm{Id}).$$

Indeed, any tensor in the image of $f \otimes \mathrm{Id}$ can be written as $\sum_i f(n_i') \otimes m$. Applying $g \otimes \mathrm{Id}$, we get

$$\sum_i g(f(n_i')) \otimes m = \sum_i 0 \otimes m = 0.$$

The only non-trivial calculation is to show that

$$\mathrm{Ker}(g \otimes \mathrm{Id}) \subset \mathrm{Im}(f \otimes \mathrm{Id}).$$

Consider a bilinear map

$$\beta : N \times M \to N \otimes_R M \to (N \otimes_R M)/\operatorname{Im}(f \otimes \mathrm{Id}),$$

where the second map is just a projection. For any $n' \in N'$, we

$$\beta(f(n'), m) = f(n') \otimes m + \mathrm{Im}(f \otimes \mathrm{Id}) = 0.$$

So $\beta$ induces a bilinear map

$$\tilde{\beta} : (N/\operatorname{Im} f) \times M \to (N \otimes_R M)/\operatorname{Im}(f \otimes \mathrm{Id})$$

by a well-defined formula

$$\tilde{\beta}(n + \operatorname{Im} f, m) := \beta(n, m).$$

Since (9) is exact, we have

$$N/\operatorname{Im} f \simeq N/\operatorname{Ker} g \simeq N''.$$

So $\tilde{\beta}$ induces a bilinear map

$$\tilde{\beta} : N'' \times M \to (N \otimes_R M)/\operatorname{Im}(f \otimes \mathrm{Id}),$$

which operates as follows: for any pair $(n'', m)$, write $n'' = g(n)$, then

$$\tilde{\beta}(n'', m) = n \otimes m + \mathrm{Im}(f \otimes \mathrm{Id}).$$

By the universal property of the tensor product, $\tilde{\beta}$ factors through the linear map

$$\tilde{B} : N'' \otimes_R M \to (N \otimes_R M)/\operatorname{Im}(f \otimes \mathrm{Id})$$

such that

$$\tilde{B}(g(n) \otimes m) = n \otimes m + \mathrm{Im}(f \otimes \mathrm{Id}).$$

The main point is that $\tilde{B}$ is a well-defined map. Here is the main calculation: take $\sum_i n_i \otimes m \in \mathrm{Ker}(g \otimes \mathrm{Id})$, i.e. $\sum_i g(n_i) \otimes m = 0$. Then

$$\tilde{B}\left(\sum_i g(n_i) \otimes m\right) = \tilde{B}(0) = 0.$$

But on the other hand,

$$\tilde{B}(\sum_i g(n_i) \otimes m) = \sum_i \tilde{B}(g(n_i) \otimes m) = \sum_i n_i \otimes m + \mathrm{Im}(f \otimes \mathrm{Id}).$$

It follows that

$$\sum_i n_i \otimes m \in \mathrm{Im}(f \otimes \mathrm{Id}),$$

and so $\mathrm{Ker}(g \otimes \mathrm{Id}) \subset \mathrm{Im}(f \otimes \mathrm{Id})$. □

Right-exactness is a very useful tool for computing tensor products.

PROPOSITION 2.5.4. *Suppose $N$ is a finitely presented $R$-module, i.e. we have an exact sequence*

$$R^n \xrightarrow{A} R^m \to N \to 0,$$

*where $A$ is an $m \times n$ matrix of elements of $R$. Then*

$$N \otimes M \simeq M^m / \operatorname{Im}[M^n \xrightarrow{A} M^m],$$

*where an $R$-linear map $A : M^n \xrightarrow{A} M^m$ just multiplies a column vector of $n$ elements of $M$ by a matrix $A$.*

*Proof.* This immediately follows from Lemma 2.5.2 and right-exactness of a tensor product. Indeed, exactness of the presentation of $N$ implies exactness of the sequence

$$M^n \xrightarrow{A} M^m \to N \otimes M \to 0$$

and Proposition follows. □

EXAMPLE 2.5.5. Let's compute $\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Z}_9$. Take a presentation for $\mathbb{Z}_6$:

$$\mathbb{Z} \xrightarrow{\cdot 6} \mathbb{Z} \to \mathbb{Z}_6 \to 0$$

and tensor it with $\mathbb{Z}_9$:

$$\mathbb{Z}_9 \xrightarrow{\cdot 6} \mathbb{Z}_9 \to \mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Z}_9 \to 0.$$

So $\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Z}_9$ is isomorphic to the quotient of $\mathbb{Z}_9$ by a submodule of multiples of 6. Since $g.c.d.(6,9) = 3$, this is the same thing as the quotient of $\mathbb{Z}_9$ by a submodule of multiples of 3. So

$$\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Z}_9 \simeq \mathbb{Z}_9 / 3\mathbb{Z}_9 \simeq \mathbb{Z}_3.$$

§2.6. **Restriction of scalars.** Recall that if $V$ is a complex vector space, we can also consider $V$ as a real vector space by "forgetting" how to multiply by $i \in \mathbb{C}$. This gives a forgetful functor

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

called restriction of scalars. Restriction of scalars doubles dimension: if $\{e_1, \dots, e_n\}$ is a basis of $V$ (over $\mathbb{C}$) then the basis of $V$ over $\mathbb{R}$ is given by

$$\{e_1, \dots, e_n, ie_1, \dots, ie_n\}$$

We can define restriction of scalars in a much broader setting of modules. Consider an arbitrary homomorphism of rings

$$f : R \to S$$

(in the example above, this is just an inclusion of fields $\mathbb{R} \hookrightarrow \mathbb{C}$). Suppose $M$ is an $S$-module. We claim that we can also view $M$ as an $R$-module, by keeping an old structure of an Abelian group on $M$, and defining an action of an element $r \in R$ on $m \in M$ by formula

$$(r, m) \mapsto f(r)m.$$

It is easy to see that this endows $M$ with a structure of an $R$-module: an expression $f(r)m \in M$ is bilinear in both $r$ and $m$, and also we have

$$f(r_1 r_2)m = [f(r_1)f(r_2)]m = f(r_1)\left(f(r_2)m\right).$$

Also, for any $S$-linear map of $S$-modules $M_1 \to M_2$, the same map is also automatically $R$-linear, and so we get a "restriction of scalars" functor

$$\mathbf{Mod}_S \to \mathbf{Mod}_R\,.$$

EXAMPLE 2.6.1. The map $\mathbb{R} \hookrightarrow \mathbb{C}$ is an inclusion, but restriction of scalars is also very interesting in the opposite case when $f : R \to S$ is surjective, i.e. when $S \simeq R/I$, where $I \subset R$ is some ideal. We can ask, which $R$-modules can be obtained by restricting of scalars from $R/I$-modules? In other words, which $R$-modules $M$ can also be viewed as $R/I$-modules? The condition is simple: $I$ should act trivially on $M$, i.e. we should have $rm = 0$ for any $r \in I$, $m \in M$. For example, modules over $\mathbb{Z}/4\mathbb{Z}$ can be identified with $\mathbb{Z}$-modules (i.e. Abelian groups) where $4$ acts trivially. For instance, if this module is finitely generated, then the structure theorem of finitely generated Abelian groups implies that $M$ is a direct sum of several copies of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$.

§2.7. **Extension of scalars.** Going back to complex and real vector spaces, we have a much more interesting functor

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

called *complexification*, or extension of scalars, which is defined as follows. For any vector space $V$ over $\mathbb{R}$, consider the set of pairs of vectors $(v_1, v_2)$, which we are going to write as "formal" linear combinations $v_1 + iv_2$, and define the multiplication by $r = a + bi \in \mathbb{C}$ as usual:

$$(a + bi)(v_1 + iv_2) = (av_1 - bv_2) + i(av_2 + bv_1).$$

It is easy to see that this gives a vector space $V_{\mathbb{C}}$ over $\mathbb{C}$ called complexification of $V$. For example, if $V$ is a vector space of real column vectors then $V_{\mathbb{C}}$ is a vector space of complex column-vectors.

Moreover, for any $\mathbb{R}$-linear map $V \xrightarrow{f} V'$, we have an induced $\mathbb{C}$-linear map $V_{\mathbb{C}} \to V'_{\mathbb{C}}$ that sends $v_1 + iv_2$ to $f(v_1) + if(v_2)$. So the complexification is indeed a functor $\mathbf{Vect}_{\mathbb{R}} \to \mathbf{Vect}_{\mathbb{C}}$. Notice that if $\{e_1, \dots, e_n\}$ is a basis of $V$ (over $\mathbb{R}$) then $\{e_1, \dots, e_n\}$ is also a basis of $V_{\mathbb{C}}$ (over $\mathbb{C}$), i.e. complexification preserves dimensions. However, the basis of $V_{\mathbb{C}}$ over $\mathbb{R}$ is equal to $\{e_1, \dots, e_n, ie_1, \dots, ie_n\}$, and so $V_{\mathbb{C}}$ over $\mathbb{R}$ has the same dimension as the tensor product $V \otimes_{\mathbb{R}} \mathbb{C}$, because $\mathbb{C}$ (as a vector space over $\mathbb{R}$) has basis $\{1, i\}$. In fact, $V_{\mathbb{C}}$ (as a real vector space) is isomorphic to $V \otimes_{\mathbb{R}} \mathbb{C}$. This isomorphism is independent of the choice of basis and simply takes $v_1 + iv_2$ to $v_1 \otimes 1 + v_2 \otimes i$. However, $V \otimes_{\mathbb{R}} \mathbb{C}$ is just a real vector space but $V_{\mathbb{C}}$ is a complex vector space. Is it possible to introduce the structure of a compex vector space on $V \otimes_{\mathbb{R}} \mathbb{C}$ directly?

We will see that this is easy, and can be done in a framework of modules. Consider an arbitrary homomorphism of rings

$$f : R \to S$$

(in the example above, this was an inclusion of fields $\mathbb{R} \hookrightarrow \mathbb{C}$). Suppose $M$ is an $R$-module and we want to construct an $S$-module. First of all, notice that $S$, as any other $S$-module, can be viewed as an $R$-module by "restriction of scalars" construction above. So we can form a tensor product

$$M \otimes_R S$$

This is not yet what we want, because $M \otimes_R S$ is an $R$-module, but we want an $S$-module. So we are going to define the action of $S$ on $M \otimes_R S$ by, as usual, defining it on pure tensors first by formula

$$(s, m \otimes s') \mapsto m \otimes (ss')$$

LEMMA 2.7.1. *This gives a well-defined $S$-module structure on $M \otimes_R S$, called the extension of scalars from $M$.*

*Proof.* Why is this well-defined? Consider an $R$-bilinear map

$$M \times S \to M \otimes_R S, \quad (m, s') \mapsto m \otimes (ss')$$

By linear extension, it gives an $R$-linear map

$$M \otimes_R S \to M \otimes_R S, \quad m \otimes s' \mapsto m \otimes (ss'),$$

which is exactly what we want.

The only thing to check is that this indeed gives an action of $S$, i.e. that all axioms of an $S$-module are satisfied. Our action on arbitrary tensors is

$$\left(s, \sum_i m_i \otimes s_i'\right) \mapsto \sum_i m_i \otimes (ss_i').$$

This is bilinear both in $s$ and in linear combinations $\sum_i m_i \otimes s_i'$. Finally, we have to check that the effect of multiplying by $s_1 s_2$ is the same as multiplying by $s_2$ and then multiplying by $s_1$. This is clear. □

§2.8. **Exercises.** In this worksheet, $k$ is a field, $R$ is a commutative ring, and $p$ is a prime.

**1.** (a) Let $n, m \in \mathbb{Z}$ and let $d$ be their g.c.d. Prove that

$$(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z}.$$

(b) Let $R$ be a PID, let $x, y \in R$, and let $d$ be their g.c.d. Prove that

$$(R/(x)) \otimes_R (R/(y)) \simeq R/(d).$$

**2.** An $R$-module $M$ is called flat, if for any short exact sequence

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

of $R$-modules, a sequence

$$0 \to N' \otimes M \to N \otimes M \to N'' \otimes M \to 0$$

is also exact. Classify all finitely generated flat $\mathbb{Z}$-modules.

**3.** Let $V$ be a vector space over $k$. Show that $V$ is a flat $k$-module.

**4.** Let $M$ be an $R$-module and let $I \subset R$ be an ideal. Prove that

$$M \otimes_R (R/I) \simeq M/(IM).$$

**5.** Compute $(x, y) \otimes_{k[x,y]} \big(k[x, y]/(x, y)\big)$.

**6.** Let $R \to S$ be a homomorphism of rings and let $M, N$ be two $S$-modules. By restriction of scalars, we can also view $M$ and $N$ as $R$-modules. Show that if $M \otimes_R N = 0$ then $M \otimes_S N = 0$. Is the converse true?

**7.** Let $M$ and $N$ be finitely generated modules over the ring of power series $k[[x]]$. Show that if $M \otimes_{k[[x]]} N = 0$ then either $M = 0$ or $N = 0$.

**8.** Consider linear maps of $k$-vector spaces $A : U \to V$ and $A' : U' \to V'$. We define their tensor product $A \otimes A'$ to be a linear map $U \otimes_k U' \to V \otimes V'$ such that

$$(A \otimes A')(u \otimes u') = A(u) \otimes A(u').$$

(a) Show that $A \otimes A'$ is well-defined. (b) Compute the Jordan normal form of $A \otimes A'$ if $A$ and $A'$ both have Jordan form $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. (c) Give a general formula for $\mathrm{Tr}(A \otimes A')$.

**9.** Let $V$ be a finite-dimensional vector space and let $V^*$ be its dual space. Construct a canonical isomorphism (independent of the basis) between (a) $V^* \otimes V^*$ and the vector space of bilinear maps $V \times V \to k$; (b) $V^* \otimes V$ and the vector space of linear maps $V \to V$.

**10.** Let $M, N$ be two $R$-modules. Let $\mathrm{Hom}_R(M, N)$ be the set of $R$-linear maps $M \to N$. (a) Show that $\mathrm{Hom}_R(M, N)$ is an $R$-module. (b) Show that $\mathrm{Hom}(\cdot, M)$ is a left-exact contravariant functor from the category of $R$-modules to itself.

**11.** Let $M_1, M_2, M_3$ be $R$-modules. Construct a canonical isomorphism between $(M_1 \otimes_R M_2) \otimes_R M_3$ and $M_1 \otimes_R (M_2 \otimes_R M_3)$. Describe a covariant functor represented by this module without using a word "tensor".

**12.** Let $R$ be a ring. An $R$-algebra $S$ is a data that consists of a ring $S$ and a homomorphism of rings $R \to S$. Then $S$ is both a ring and an $R$-module (by restriction of scalars). For example, $k[x]$ is a $k$-algebra. (a) Show that if $S_1, S_2$ are two $R$-algebras then $S_1 \otimes_R S_2$ is also an $R$-algebra such that

$$(s_1 \otimes s_2)(s_1' \otimes s_2') = (s_1 s_1') \otimes (s_2 s_2')$$

(check that this multiplication is well-defined, satisfies all axioms of a commutative ring with 1, and there is a natural homomorphism $R \to S_1 \otimes_R S_2$.) (b) Prove that $k[x] \otimes_k k[y] \simeq k[x, y]$.

**13.** Construct a non-trivial Abelian group $M$ such that $M \otimes_{\mathbb{Z}} M = 0$.

**14.** For any $R$-modules $M_1$, $M_2$, and $N$, construct a canonical isomorphism between $(M_1 \oplus M_2) \otimes_R N$ and $(M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$. Generalize to arbitrary direct sums (with more than two summands).

## §3. Algebraic Extensions

§3.1. **Field Extensions.** Let $K \subset F$ be fields. Then $F$ is called a *field extension* of $K$. Examples: $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$, etc.

Definition 3.1.1. An element $\alpha \in F$ is called *algebraic* over $K$ if $\alpha$ is a root of a non-constant polynomial with coefficients in $K$. An element $\alpha$ is called *transcendental* if it is not algebraic.

- $i \in \mathbb{C}$ is a root of $x^2 - 1$, so $i$ is algebraic over $\mathbb{Q}$.
- $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$ (Lindemann's Theorem).
- $x \in \mathbb{C}(x)$ is transcendental over $\mathbb{C}$ (obvious).

Definition 3.1.2. Let $\alpha \in F$ be algebraic. A polynomial $f(x) \in K[x]$ is called a *minimal polynomial* of $\alpha$ if $f(x)$ is a monic non-costant polynomial of minimal degree such that $f(\alpha) = 0$.

Let us point out one persistent notational ambiguity. If $x$ is a variable then $K[x]$ denotes the algebra of polynomials and $K(x)$ denotes the field of rational functions (i.e. ratios of polynomials) in variable $x$. But if $\alpha \in F$ then $K[\alpha]$ denotes the minimal subring of $F$ generated by $K$ and by $\alpha$ and $K(\alpha)$ denotes the minimal subfield of $F$ generated by $K$ and by $\alpha$. These objects are related as follows:

THEOREM 3.1.3. *Let $\alpha \in F$. We have a unique surjective homomorphism*

$$\phi : K[x] \to K[\alpha]$$

*that sends $x$ to $\alpha$. If $\alpha$ is algebraic then $\operatorname{Ker}\phi$ is generated by the minimal polynomial $f(x)$, which is unique and prime. In this case the map $\phi$ does not extend to the map $K(x) \to K(\alpha)$. In fact, in this case $K(\alpha) = K[\alpha]$ is finite-dimensional over $K$ and elements $1, \alpha, \dots, \alpha^{n-1}$ form a basis, where $n = \deg(x)$.*

*If $\alpha$ is transcendental then $\phi$ is an isomorphism, which induces an isomorphism of fields $K(x) \simeq K(\alpha)$.*

*Proof.* $\operatorname{Ker}\phi$ is an ideal of all polynomials that vanish at $\alpha$. $\operatorname{Ker}\phi = 0$ if and only if $\alpha$ is transcendental (by definition). In this case

$$K[x] \simeq K[\alpha] \subset F.$$

Any injective homomorphism of a domain into a field extends to the inhective homomorphism of its field of fractions. So in our case $\phi$ extends to the injective homomorphism $K(x) \to F$, and its image is obviously $K(\alpha)$.

If $\alpha$ is algebraic then, since $K[x]$ is a PID, $\operatorname{Ker}\phi$ is generated by a unique monic polynomial $f(x)$, hence a minimal polynomial is unique. Since

$$K[x]/\operatorname{Ker}\phi \simeq K[\alpha]$$

injects in $F$, which is a domain, $K[x]/\operatorname{Ker}\phi$ is also a domain, hence $f(x)$ is irreducible and $\operatorname{Ker}\phi = (f)$ is a maximal ideal. Hence $K[x]/Ker\phi$ is a field. Therefore, $K[\alpha]$ is a field. Therefore, $K[\alpha] = K(\alpha)$.

Finally, we notice that $1, \alpha, \dots, \alpha^{n-1}$ are linearly independent over $K$ (otherwise we can find a smaller degree polynomial vanishing at $\alpha$) and span $K[\alpha]$ over $K$. Indeed, since $f(x) = x^n + \dots$ vanishes at $\alpha$, we can rewrite $\alpha^n$ as a linear combination of smaller powers of $\alpha$. Then, an easy argument by induction shows that we can rewrite any $\alpha^m$ for $m > n$ as as a linear combination of $1, \alpha, \dots, \alpha^{n-1}$. □

DEFINITION 3.1.4. The dimension $\dim_K F$ is called the *degree* of $F$ over $K$. Notation: $[F : K]$. For example, $[\mathbb{C} : \mathbb{R}] = 2$. If $[F : K] < \infty$ then $F$ is called a *finite extension* of $K$. An extension $K \subset F$ is called *algebraic* if any element of $F$ is algebraic over $K$.

COROLLARY 3.1.5. *If $\alpha$ is algebraic over $K$ then $[K(\alpha) : K]$ is equal to the degree of the minimal polynomial of $\alpha$.*

LEMMA 3.1.6. *Consider a tower of field extensions*

$$K \subset F \subset L.$$

*If $[F : K] = n$ and $[L : F] = m$ then $[L : K] = nm$.*

*Proof.* It is easy to prove a bit more: if $e_1, \dots, e_m$ is a basis of $L$ over $F$ and $f_1, \dots, f_n$ is a basis of $F$ over $K$ then $\{e_i f_j\}$ is a basis of $L$ over $K$. □

THEOREM 3.1.7. *(a) Any finite extension is algebraic.*
*(b) Let $\alpha_1, \dots, \alpha_r \subset F$ be algebraic over $K$. Then*

$$K(\alpha_1, \dots, \alpha_r) = K[\alpha_1, \dots, \alpha_r]$$

*is finite over $K$. In particular, any element of $K(\alpha_1, \dots, \alpha_r)$ is algebraic over $K$.*

*Proof.* If $[F : K] < \infty$ then $1, \alpha, \alpha^2, \dots$ are linearly dependent over $K$ for any $\alpha \in F$. Therefore, some non-constant polynomial with coefficient in $K$ vanishes at $\alpha$, i.e. $\alpha$ is algebraic.

Now suppose that $\alpha_1, \dots, \alpha_r \subset F$ are algebraic over $K$. Arguing by induction (with the base of induction given by Theorem 3.1.3), let's assume that $K(\alpha_1, \dots, \alpha_{r-1}) = K[\alpha_1, \dots, \alpha_{r-1}]$ is finite over $K$. Since $\alpha_r$ is algebraic over $K$, it is also algebraic over $K(\alpha_1, \dots, \alpha_{r-1})$. Using Theorem 3.1.3, we see that

$$K(\alpha_1, \dots, \alpha_{r-1})[\alpha_r] = K(\alpha_1, \dots, \alpha_{r-1})(\alpha_r) = K(\alpha_1, \dots, \alpha_{r-1}, \alpha_r)$$

is finite-dimensional over $K(\alpha_1, \dots, \alpha_{r-1})$. Then $[K(\alpha_1, \dots, \alpha_r) : K] < \infty$ by Lemma 3.1.6. The last statement of part (b) follows from part (a). □

§3.2. **Adjoining roots.** In the previous section we studied a fixed extension $K \subset F$. If $\alpha \in F$ is algebraic over $K$ then $K(\alpha)$ is isomorphic to $K[x]/(f)$, where $f(x)$ is a minimal polynomial of $\alpha$. An algebraic extension $K \subset K(\alpha)$ generated by one element is sometimes called *simple*.

Now we will start with a field $K$ and learn how to build its extensions and compare them. The main building block is the same:

LEMMA 3.2.1. *If $f(x) \in K[x]$ is irreducible and monic then $K[x]/(f)$ is a field extension of $K$ generated by $\alpha := x + (f)$. The minimal polynomial of $\alpha$ is $f(x)$.*

*Proof.* Since $f$ is irreducible and $K[x]$ is a PID, $K[x]/(f)$ is a field. It is obviously generated by $\alpha$. Since $f(x) \equiv 0 \mod (f)$, $\alpha$ is a root of $f(x)$. Since $f(x)$ is irreducible over $K$, $f(x)$ is the minimal polynomial of $\alpha$. □

We will often want to compare two extensions $F$ and $F'$ of the same field. We say that $F$ and $F'$ are *isomorphic over $K$* if there exists an isomorphism $\phi : F \to F'$ such that $\phi(a) = a$ for any $a \in K$. Here is the basic fact:

LEMMA 3.2.2. *Let $K(\alpha)$ and $K(\beta)$ be algebraic extensions of $K$ such that $\alpha$ and $\beta$ have the same minimal polynomial. Then $K(\alpha)$ is isomorphic to $K(\beta)$ over $K$.*

*Proof.* The analysis above shows that both of these fields are isomorphic to $K[x]/(f)$, where $f(x)$ is the common minimal polynomial. Notice that an induced isomorphism between $K(\alpha)$ and $K(\beta)$ simply sends $\alpha$ to $\beta$. □

EXAMPLE 3.2.3. Fields $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\omega\sqrt[3]{2})$ are isomorphic (here $\omega$ is a primitive cubic root of unity), because they have the same minimal polynomial $x^3 - 2$. However, they are not equal inside $\mathbb{C}$ because $\mathbb{Q}(\sqrt[3]{2})$ is contained in $\mathbb{R}$ but the other field is not.

Next we would like to adjoin all roots of a polynomial.

DEFINITION 3.2.4. A field $F \supset K$ is called a *splitting field* of $f(x) \in K[x]$ if

- $f$ splits into linear factors in $F[x]$, and
- $F$ is generated by roots of $f(x)$.

In other words, $f(x)$ splits in $F$ but not in any proper subfield of $F$.

LEMMA 3.2.5. *Any polynomial $f(x) \in K[x]$ has a splitting field. Moreover, any two splitting fields $L$ and $L'$ are isomorphic over $K$.*

*Proof.* Existence is proved by induction on $\deg f$: if $f(x)$ does not split then it has an irreducible factor $g(x)$ of degree greater than one. Lemma 3.2.1 gives an extension $K \subset L = K(\alpha)$ such that $g(x)$ has a root $\alpha \in L$. Then $f(x)/(x-\alpha) \in L[x]$ has a splitting field $F \supset L$ by inductive assumption. Then $F$ is a splitting field of $f(x) \in K[x]$ as well.

Now we have to construct an isomorphism between two splitting fields $L$ and $L'$ over $K$. It is enough to construct an injective homomorphism $\phi : L \to L'$ that preserves $K$. Indeed, if $f(x) = c\prod_i(x-\alpha_i)$ in $L$ then $f(x) = \phi(c)\prod_i(x-\phi(\alpha_i))$ in $\phi(L)$, so $f(x)$ splits in $\phi(L)$, so $\phi(L) = L'$.

We will construct $\phi$ step-by-step. Choose a root $\alpha \in L$ of $f(x)$. Let $g(x)$ be the minimal polynomial of $\alpha$. Then $g(x)$ divides $f(x)$, and in particular $g(x)$ splits in $L'$. Let $\beta$ be a root of $g(x)$ in $L'$. Since $\alpha$ and $\beta$ have the same minimal polynomial, $K(\alpha)$ and $K(\beta)$ are isomorphic over $K$. Fix one isomorphism,

$$\phi_0 : K(\alpha) \to K(\beta).$$

Now we have a diagram of field maps

$$\begin{array}{ccc} L & & L' \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow[\phi_0]{} & K(\beta) \end{array} \tag{1}$$

Notice that $L$ is a splitting field of $f(x)$ over $K(\alpha)$ and $L'$ is a splitting field of $f(x)$ over $K(\beta)$. So ideally, we would like to finish by induction by continuing to add roots of $\alpha$. However, notice that the set-up is slightly different: before we were trying to show that $L$ and $L'$ are isomorphic over $K$, and now we are trying to construct an isomorphism $\phi : L \to L'$ that extends a given isomorphism $\phi_0 : K(\alpha) \to K(\beta)$. So the best thing to do is to generalize our Lemma a little bit to make it more suitable for induction. This is done in the next Lemma. □

LEMMA 3.2.6. *Suppose we have a diagram of homomorphisms of fields*

$$\begin{array}{ccc} L_1 & & L_2 \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow[\psi]{} & K_2 \end{array} \tag{2}$$

*where $L_1$ is a splitting field of $f_1(x) \in K_1[x]$, the polynomial $f_2(x) \in K_2[x]$ splits in $L_2$, and $f_2(x)$ is a polynomial obtained by applying $\psi$ to all coefficients of $f_1(x)$. Then there exists a homomorphism $\phi : L_1 \to L_2$ such that $\phi|_{K_1} = \psi$ (i.e. that makes a diagram commutative).*

*Proof.* Choose a root $\alpha \in L_1$ of $f_1(x)$. Let $g_1(x)$ be the minimal polynomial of $\alpha$. Then $g_1(x)$ divides $f_1(x)$. We have a homomorphism

$$\Psi : K_1[x] \to K_2[x]$$

that extends $\psi$. Then $f_2 = \Psi(f_1)$. Let $g_2 = \Psi(g_1)$. Then $g_2|f_2$, and in particular $g_2(x)$ splits in $L_2$. Let $\beta$ be a root of $g_2(x)$ in $L_2$. Let $g_2'(x) \in K_2[x]$ be an irreducible factor of $g_2(x)$ with root $\beta$. Then

$$K_1(\alpha) \simeq K_1[x]/(g_1) \quad \text{and} \quad K_2(\beta) \simeq K_2[x]/(g_2').$$

Notice that $\Psi$ induces a homomorphism $K_1[x]/(g_1) \to K_2[x]/(g_2')$. This gives an homomorphism

$$\phi_0 : K_1(\alpha) \to K_2(\beta)$$

that sends $\alpha$ to $\beta$ and such that $\phi_0|_{K_1} = \psi$. Now we have a commutative diagram of field maps

$$\begin{array}{ccc} L_1 & & L_2 \\ \uparrow & & \uparrow \\ K_1(\alpha) & \xrightarrow[\phi_0]{} & K_2(\beta) \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow[\psi]{} & K_2 \end{array} \tag{3}$$

Notice that $L_1$ is a splitting field of $f_1(x)$ over $K_1(\alpha)$ and $L_2$ is a splitting field of $f_2(x)$ over $K_2(\beta)$. So we are in the same set-up as in the statement of the Lemma, but now $[L_1 : K_1(\alpha)] < [L_1 : K_1]$. So we can finish by induction on $[L_1 : K_1]$. □

## §3.3. **Algebraic Closure.**

LEMMA 3.3.1. *Let $K$ be a field. The following are equivalent:*

- *any polynomial $f \in K[x]$ has a root in $K$.*
- *any polynomial $f \in K[x]$ splits in $K$.*
- *The only algebraic extension of $K$ is $K$ itself.*

*Proof.* Easy. □

If any of these conditions are satisfied then $K$ is called *algebraically closed*.

DEFINITION 3.3.2. Le $K$ be a field. A field $\bar{K}$ containing $K$ is called an *algebraic closure* of $K$ if

- $\bar{K}$ is algebraically closed.
- $K \subset \bar{K}$ is an algebraic extension.

For example, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$ but not of $\mathbb{Q}$.

LEMMA 3.3.3. *Let $K \subset F$ be a field extension with $F$ algebraically closed. Then*

$$\bar{K} = \{a \in F \,|\, a \text{ is algebraic over } F\}$$

*is an algebraic closure of $K$.*

*Proof.* If $\alpha, \beta \in \bar{K}$ then $K(\alpha, \beta)$ is finite algebraic over $K$. In particular, $\bar{K}$ is a field (obviously algebraic over $K$). Any polynomial $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ in $\bar{K}[x]$ has a root $\alpha \in F$. Then $K(a_1, \ldots, a_n)$ is finite over $K$, $K(a_1, \ldots, a_n)(\alpha)$ is finite over $K(a_1, \ldots, a_n)$. Therefore, $[K(\alpha) : K] < \infty$ and $\alpha$ is algebraic. □

For example, if $K = \mathbb{Q}$ and $F = \mathbb{C}$ then $\bar{K} = \bar{\mathbb{Q}}$, the field of all algebraic numbers.

LEMMA 3.3.4. *Any field $K$ is contained in a field $F$ such that any polynomial in $K[x]$ has a root in $F$.*

*Proof.* The idea is to adjoin roots of all polynomials at once. Let $K[x_f]$ be the algebra of polynomials in variables $x_f$, one variable for each irreducible polynomial with coefficients in $K$. Consider the ideal

$$I = \langle f(x_f) \rangle$$

with one generator for each irreducible polynomial $f$. Notice that each polynomial is a polynomial in its own variable. We claim that $I$ is a proper ideal. If not, then we can write

$$1 = \sum_{i=1}^{s} g_i f_i(x_{f_i}),$$

where $g_i$ are some polynomials that involve only finitely many variables $x_f$. Let $L$ be a splitting field of the product $f_1 \dots f_s$. The formula above remains valid in $L[x_f]$. However, if we plug-in any root of $f$ for $x_f$, we will get $1 = 0$, a contradiction. It follows that $I$ is a proper ideal.

Let $M$ be a maximal ideal containing $I$. Then $F := K[x_f]/M$ is a field that contains $K$. We claim that any irreducible polynomial $f \in K[x]$ has a root in $F$. Indeed, $f(x_f) \in M$, and therefore $x_f + M$ is a root of $f$ in $F$. □

THEOREM 3.3.5. *Any field $K$ has an algebraic closure. It is unique up to an isomorphism over $K$.*

*Proof.* Applying Lemma 3.3.4 inductively gives an infinite tower of fields

$$K = F_0 \subset F_1 \subset F_2 \subset \dots$$

such that any polynomial in $F_k[x]$ has a root in $F_{k+1}$. Then $F = \cup_i F_i$ is algebraically closed as any polynomial in $F[x]$ in fact belongs to some $F_k[x]$, and therefore has a root in $F$. Applying Lemma 3.3.3 gives an algebraic closure $\bar{K}$.

Let $\bar{K}$, $\bar{K}_1$ be two algebraic closures of $K$. It suffices to show that there exists a homomorphism $\phi : \bar{K} \to \bar{K}_1$ over $K$. Indeed, $\phi(\bar{K})$ is then another algebraic closure of $K$ contained in $\bar{K}_1$. Since $\bar{K}_1$ is algebraic over $\phi(\bar{K})$, it must be equal to it.

Finally, we construct $\phi$ using Zorn's lemma. Consider a poset of pairs $(F, \phi)$, where $K \subset F \subset \bar{K}$ and $\phi : F \to \bar{K}_1$ is a homomorphism over $K$. We say that $(F, \phi) \leq (F_1, \phi_1)$ if $F \subset F_1$ and $\phi$ is the restriction of $\phi_1$ to $F$. Then any chain has a maximal element $(F, \phi)$ (take the union of fields in the chain and the map $\phi$ induced by maps in the chain). This maximal field must be equal to $\bar{K}$: if $F$ is properly contained in $\bar{K}$ then take any $\alpha \in \bar{K} \setminus F$.

By Lemma 3.2.6, we can extend $\phi$ to a homomorphism $F(\alpha) \to \bar{K}_1$. □

The same argument shows the following slightly more useful statement:

PROPOSITION 3.3.6. *Suppose we have a diagram of homomorphisms of fields*

$$\begin{array}{ccc} & & L_1 \\ & & \uparrow \\ K_1 & \xrightarrow[\psi]{} & K_2 \end{array} \tag{4}$$

*where $L_1$ is algebraic over $K_1$ and $K_2$ is algebraically closed. Then there exists a homomorphism $\phi : L_1 \to K_2$ such that $\phi|_{K_1} = \psi$ (i.e. that makes a diagram commutative).*

## §3.4. **Finite Fields.**

THEOREM 3.4.1. *For any prime $p$ and positive integer $n$, there exists a field $\mathbb{F}_{p^n}$ with $p^n$ elements. Moreover, any two such fields are isomorphic. We can embed $\mathbb{F}_{p^m}$ in $\mathbb{F}_{p^n}$ if and only if $m$ divides $n$.*

*Proof.* Let $K$ be a splitting field of the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Since $f'(x) = -1$ is coprime to $f(x)$, there are exactly $p^n$ roots. Recall that $F : K \to K$, $F(x) = x^p$ is a Frobenius homomorphism. In particular, if $\alpha$ and $\beta$ are roots of $f(x)$ then $\pm\alpha \pm \beta$ and $\alpha\beta$, and $\alpha/\beta$ are roots as well. It follows that $K$ has $p^n$ elements and all of them are roots of $f(x)$.

Suppose $K$ is a field with $p^n$ elements. The group of units $K^*$ is Abelian of order $p^n - 1$, and therefore $x^{p^n-1} = 1$ for any $x \in K^*$.[1] It follows that $K$ is a splitting field of $x^{p^n} - x$. But any two splitting fields of the same polynomial are isomorphic by Lemma 3.2.5.

If $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ then the latter field is a vector space (of some dimension $r$) over the former. It follows that

$$p^n = (p^m)^r = p^{mr}.$$

It follows that $m$ divides $n$.

Finally, suppose that $m$ divides $n$. Then $p^m - 1 | p^n - 1$ (easy), and therefore $x^{p^m-1} - 1 x^{p^n-1} - 1$ (equally easy). It follows that the splitting field of $x^{p^m} - x$ is contained in the splitting field of $x^{p^n} - x$. □

## §3.5. **Exercises.**

In this set we fix a field extension $K \subset F$.

**1.** Let $R$ be an infinite domain and let $f \in R[x]$. Prove that $f(r) \neq 0$ for infinitely many $r \in R$. What if $R$ is not necessarily a domain?

**2.** (a) Show $\alpha \in F$ is algebraic over $K$ if and only if $F$ contains a finite-dimensional $K$-vector subspace $L$ (not necessarily a subfield) such that

$$\alpha \cdot L \subset L.$$

(b) Find the minimal polynomial of $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$.

**3.** (a) Let $R$ be a domain and let $R \subset K$ be its field of fractions. Show that $K$ satisfies the following universal property: for any injective homomorphism $\psi : R \to F$ to a field, there exists a unique homomorphism of fields $K \to F$ that extends $\psi$. (b) Let **Fields** be the category of fields (what can you

[1] Recall that in fact this analysis implies that $K^*$ is a cyclic group. Indeed, otherwise we would have $x^r = 1$ for any $x \in K^*$ and $r < p^n - 1$. However, the polynomial can not have more roots than its degree.

say about morphisms in this category?). Let $R$ be a domain and let $F_R$ : **Fields** $\to$ **Sets** be a covariant functor that sends any field $k$ to the set of injective homomorphisms $R \to k$. This definition is not complete: give a complete definition of this functor and show that it is representable.

**4.** (a) Show that $f(x) = x^3 + x^2 + x + 3$ is irreducible over $\mathbb{Q}$. (b) Consider the field $F = K(\alpha)$, where $\alpha$ is a root of $f(x)$. Express $\frac{1}{2-\alpha+\alpha^2}$ as a $\mathbb{Q}$-linear combination of $1$, $\alpha$, and $\alpha^2$.

**5.** Find the degree (over $\mathbb{Q}$) of the splitting field of (a) $x^4 + x^3 + x^2 + x + 1$. (b) $x^4 - 2$.

**6.** For all positive integers $n$ and $m$, compute the degree $[\mathbb{Q}(\sqrt{n}, \sqrt{m}) : \mathbb{Q}]$.

**7.** Let $K \subset F$ be an algebraic extension and let $R$ be a subring of $F$ that contains $K$. Show that $R$ is a field.

**8.** Let $f(x) \in K[x]$ be a polynomial of degree 3. Show that if $f(x)$ has a root in a field extension $K \subset F$ of degree 2 then $f(x)$ has a root in $K$.

**9.** Let $\alpha, \beta \in F$ be algebraic over $K$, let $f(x)$ and $g(x)$ be their minimal polynomials, and suppose that $\deg f$ and $\deg g$ are coprime. Prove that $f(x)$ is irreducible in $K(\beta)[x]$.

**10.** Find the splitting field of $x^p - 1$ over $\mathbb{F}_p$.

**11.** Let $K \supset \mathbb{Q}$ be a splitting field of a cubic polynomial $f(x) \in \mathbb{Q}[x]$. Show that if $[K : \mathbb{Q}] = 3$ then $f(x)$ has 3 real roots.

**12.** Let $\mathbb{F}_{p^n}$ be a finite field with $p^n$ elements and let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the Frobenius map, $F(x) = x^p$. Show that $F$ is diagonalizable (as an $\mathbb{F}_p$-linear operator) if and only if $n$ divides $p - 1$.

**13.** Let $F = K(\alpha)$ and suppose that $[F : K]$ is odd. Show that $F = K(\alpha^2)$.

**14.** Let $f(x) \in K[x]$ be an irreducible polynomial and let $g(x) \in K[x]$ be any non-constant polynomial. Let $p(x)$ be a non-constant polynomial that divided $f(g(x))$. Show that $\deg f$ divides $\deg p$.

**15.** Show that the polynomial $x^5 - t$ is irreducible over the field $\mathbb{C}(t)$ (here $t$ is a variable). Describe a splitting field.

**16.** Let $\mathbb{F}_q$ be a finite field with $q$ elements ($q$ is not necessarily prime). Compute the sum $\sum_{a \in \mathbb{F}_q} a^k$ for any integer $k$.

**17.** Show that the algebraic closure of $\mathbb{F}_p$ is equal to the union of its finite subfields:

$$\bar{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}.$$

## §4. GALOIS THEORY

Let $K \subset F$ be an algebraic extension. For convenience, in this section we fix an algebraic closure $\bar{K}$ of $K$ and assume that $F \subset \bar{K}$.

### §4.1. **Separable Extensions.**

DEFINITION 4.1.1. An element $\alpha \in F$ is called *separable* over $K$ if its minimal polynomial has no multiple roots.

LEMMA 4.1.2. *Let $\alpha \in F$ and let $f(x)$ be its minimal polynomial. Then $\alpha$ is not separable if and only if* $\operatorname{char} K = p$ *and $f'(x) \equiv 0$.*

*Proof.* Indeed, $f(x)$ has a multiple root if and only the g.c.d. of $f(x)$ and $f'(x)$ has positive degree. This greatest common divisor belongs to $K[x]$, and since $f(x)$ is irreducible, it is only possible if $f'(x) \equiv 0$. This implies that $\operatorname{char} K = p$ and $f(x) = g(x^p)$ for some polynomial $g(x)$. □

DEFINITION 4.1.3. An algebraic extension $F/K$ is called *separable* if any $\alpha \in F$ is separable over $K$.

THEOREM 4.1.4. *Let $F/K$ be an algebraic extension. Suppose that $F$ is generated over $K$ by elements $\alpha_i$, $i \in I$. Then the following conditions are equivalent:*

(1) *$F/K$ is separable.*
(2) *$\alpha_i$ is separable for any $i \in I$.*

*If, in addition, $F/K$ is finite then this is equivalent to*

(3) *The number of different embeddings $F \to \bar{K}$ over $K$ is equal to $[F : K]$, the maximum possible number.*

*Proof.* (1) obviously implies (2). Next we assume that $F/K$ is finite and show that (2) implies (3). In this case $F$ is generated by finitely many $\alpha_i$'s, so we can assume that $I = \{1, \ldots, r\}$ is a finite set. Then we have the tower

$$K = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_r = F,$$

where $F_k = K(\alpha_1, \ldots, \alpha_k)$. Each $\alpha_k$ is separable over $K$ and hence separable over $F_{k-1}$. We have $F_k = F_{k-1}(\alpha_k)$, and therefore the number of different embeddings of $F_k$ in $\bar{K}$ over $F_{k-1}$ is equal to $[F_k : F_{k-1}]$. But any homomorphism $F \to \bar{K}$ can be constructed step-by-step by extending the inclusion $K \subset \bar{K}$ to fields $F_k$ in the tower. It follows that the number of different embeddings $F \to \bar{K}$ over $K$ is equal to

$$[F : F_{r-1}][F_{r-1} : F_{r-2}] \ldots [F_1 : K] = [F : K].$$

Moreover, the same reasoning shows that this is the maximum possible number of embeddings.

Now we show that (3) implies (1) (still assuming that $F/K$ is finite). Suppose that $\alpha \in F$ is not separable. Then the number of embeddings $K(\alpha) \to \bar{K}$ is strictly less then $[K(\alpha) : K]$, and considering the tower $K \subset K(\alpha) \subset F$ gives the contradiction. Indeed, by the above, the number of different embeddings $F \to \bar{K}$ over $K(\alpha)$ is at most $[F : K(\alpha)]$.

Finally, we show that (2) implies (1) in general. Take $\alpha \in F$. Then $\alpha \in K(\alpha_1, \ldots, \alpha_k)$ for a finite subset of generators. Since $K(\alpha_1, \ldots, \alpha_k)$ is finite over $K$, the finite extension case considered above shows that $\alpha$ is separable. □

The following theorem is a nice bonus feature of separable extensions.

THEOREM 4.1.5 (Theorem on the Primitive Element). *If $F/K$ is a finite separable extension then $F = K(\gamma)$ for some $\gamma \in F$.*

REMARK 4.1.6. The philosophy is that (as we will see later) $F$ contains only finitely many intermediate subfields $K \subset L \subset F$. Then $F$ is a finite-dimensional $K$-vector space, and (if $K$ is an infinite field) we can take $\gamma$ to be any vector not in the union of these proper subfields $L$ (which forms a finite collection of vector subspaces of smaller dimension). For example, the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ contains only three intermediate subfields, namely $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$. So $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is generated by any element not in this union. With a little effort one can show that in fact $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. However, in general it is easier to give an *ad hoc* argument by a trick. This trick is actually very useful (see for example the proof of Noether's normalization theorem).

*Proof.* If $K$ is a finite field then $F$ is also finite and we can take $\gamma$ to be any generator of $F^*$. Suppose now that $K$ is infinite. We can argue by induction on the number of generators of $F$ over $K$ and reduce to the following statement: if $F = K(\alpha, \beta)$ then we can find $\gamma = \beta + c\alpha$ for some $c \in K$ such that $K(\alpha, \beta) = K(\gamma)$. Since $\beta = \gamma - c\alpha$, it is enough to show that $K(\alpha) \subset K(\gamma)$ for some $c \in K$.

Let $f(x)$ (resp. $g(x)$) be the minimal polynomial of $\alpha$ (resp. $\beta$). Since $F/K$ is separable, their roots $\alpha = \alpha_1, \dots, \alpha_r$ and $\beta = \beta_1, \dots, \beta_s$ (in $\bar{K}$) are not multiple.

Consider the polynomials

$$f(x), h(x) := g(\gamma - cx) \in K(\gamma)[x]$$

Clearly $\alpha$ is their common root. If $\alpha_i$, $i \geq 2$ is another common root then $\gamma - c\alpha_i = \beta_j$ for some $j$. It follows that

$$\beta + c\alpha = \beta_j + c\alpha_i,$$

and therefore

$$c = \frac{\beta_j - \beta}{\alpha - \alpha_i}.$$

There are only finitely many choice for the RHS of this equation. So it is possible to choose a different $c$. Then $\alpha$ is the only common root of $f(x)$ and $h(x)$. Since $f(x)$ has no multiple roots, the g.c.d. of $f(x)$ and $h(x)$ is equal to $x - \alpha$. It follows that $x - \alpha \in k(\gamma)[x]$. It follows that $\alpha \in k(\gamma)$. □

## §4.2. **Normal Extensions.**

DEFINITION 4.2.1. An algebraic extension $F/K$ is called *normal* if the minimal polynomial of any $\alpha \in F$ splits in $F[x]$ in the product of linear factors.

THEOREM 4.2.2. *Let $F/K$ be algebraic and suppose that $F$ Suppose that is generated over $K$ by elements $\alpha_i$, $i \in I$. Then the following conditions are equivalent:*

(1) *$F/K$ is normal.*
(2) *$F$ is the splitting field of the collection of minimal polynomials of $\alpha_i$.*
(3) *Any embedding $F \to \bar{K}$ over $K$ has image $F$.*

*Proof.* It is obvious that (1) implies (2). Let $\sigma : F \to \bar{K}$ be any homomorphism over $K$. Then $\sigma(\alpha_i)$ is a root of the minimal polynomial of $\alpha_i$ for any $i$. It follows that $\sigma(\alpha_i) \in F$ for any $\alpha_i$. Therefore $\sigma(F) \subset F$. We claim that in fact $\sigma(F) = F$. This is clear if $F/K$ is finite. But even if it is not finite, any $\alpha \in F$ is contained in the splitting field $F'$ of finitely many of $\alpha_i$'s. The argument above shows that $\sigma(F') = F'$, and therefore any $\alpha \in F$ is in the image of $\sigma$.

Finally, we show that (3) impies (1). Suppose not. Then there exists $\alpha \in F$ such that its minimal polynomial does not split in $F$. Then there exists an embedding $K(\alpha) \to \bar{K}$ with image not contained in $F$ (just send $\alpha$ to a root of the minimal polynomial not contained in $F$). This embedding can be extended to an embedding $\sigma : F \to \bar{K}$ with $\sigma(F) \not\subset \bar{K}$. □

§4.3. **Main Theorem of Galois Theory.** We say that $K \subset F$ is a *Galois extension* if it is separable and normal.

THEOREM 4.3.1. *Let $K \subset F$ be a finite Galois extension with a Galois group $G = \mathrm{Gal}(F/K)$. Then $|G| = [F : K]$ and there is an inclusion-reversing bijection*

$$\{\text{subgroups } H \subset G\} \leftrightarrow \{\text{towers } K \subset L \subset F\}$$

*Namely, a subgroup $H$ corresponds to its fixed subfield*

$$L = F^H = \{\alpha \in F \mid h(\alpha) = \alpha \text{ for any } h \in H\}$$

*and a tower $K \subset L \subset F$ corresponds to a subgroup*

$$H = \mathrm{Gal}(F/L) \subset \mathrm{Gal}(F/K) = G.$$

*Proof.* Since $F/K$ is separable, the number of homomorphisms $F \to \bar{K}$ over $K$ is equal to $[F : K]$. Since $F/K$ is normal, the image of any such homomorphism is equal to $F$. Therefore, $|G| = [F : K]$.

Next we show that $F^G = K$. Indeed, $F^G$ is clearly a field and we have

$$K \subset F^G \subset F.$$

Since $F/F^G$ is a Galois extension, we have $|\mathrm{Gal}(F/F^G)| = [F : F^G]$ by the above. But $\mathrm{Gal}(F/F^G) = \mathrm{Gal}(F/K) = G$. Therefore, $[F : F^G] = [F : K]$ and so $F^G = K$.

Now take $K \subset L \subset F$. We map it to a subgroup $H = \mathrm{Gal}(F/L)$. We have proved in the previous step (applied to the extension $L \subset F$) that $F^H = L$. It follows that the map

$$\{K \subset L \subset F\} \to \{H \subset G\}$$

is one-to-one.

It remains to show that this map is onto and that $\mathrm{Gal}(F/F^H) = H$ for any subgroup $H \subset G$. This follows from a more general Lemma below. □

LEMMA 4.3.2. *Let $F$ be any field and let $G$ be a finite group of its automorphisms. Then $F/F^G$ is a finite Galois extension with Galois group $G$.*

*Proof.* Let $\alpha \in F$ and consider its $G$-orbit

$$G \cdot \alpha = \{\alpha_1, \ldots, \alpha_r\} \quad \text{with} \quad \alpha = \alpha_1.$$

Consider the polynomial

$$f(x) = \prod_{i=1}^{r}(x - \alpha_r).$$

By Vieta formulas, its coefficients are elementary symmetric functions in $\alpha_1, \dots, \alpha_r$. Therefore, these coefficients are $G$-invariant, i.e. $f(x) \in F^G[x]$. Since the minimal polynomial of $\alpha$ over $F^G$ divides $f(x)$, $\alpha$ is separable over $F^G$. Therefore $F/F^G$ is separable. Since all roots of the minimal polynomial of $\alpha$ are among $\{\alpha_1, \dots, \alpha_r\}$, we see that $F/F^G$ is normal as well. Therefore, $F/F^G$ is Galois. Clearly, $G \subset \mathrm{Gal}(F/F^G)$. To prove the equality, it suffices to show that $[F : F^G] \leq |G|$.

By the primitive element theorem, $F = F^G(\alpha)$ for some $\alpha$. By the analysis above, the minimal polynomial of $\alpha$ has degree at most $|G|$, and therefore $[F : F^G] = [F^G(\alpha) : F^G] \leq |G|$. □

COROLLARY 4.3.3. *Let $H \subset G$ and let $L = F^H$ be the corresponding subfield. Then $H$ is a normal subgroup of $G$ if and only if $L/K$ is a normal field extension. In this case* $\mathrm{Gal}(L/K) \simeq G/H$.

*Proof.* Suppose $L/K$ is a normal extension. Then any automorphism of $F$ over $K$ preserves $L$, i.e. we have a "restriction" homomorphism

$$\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$$

and its kernel is obviously $\mathrm{Gal}(F/L)$. The restriction homomorphism is onto because any automorphism of $L/K$ can be lifted to an automorphism of $F/K$.

In the other direction, suppose $L/K$ is not a normal extension. Then there exists $g \in G$ such that $gL \neq L$. It is easy to check that $gHg^{-1}$ is a Galois group of $F/gL$. Since $gL \neq L$, it follows by the main theorem that $H \neq gHg^{-1}$, i.e. $H$ is not normal. □

REMARK 4.3.4. A simple fact that we will exploit a lot is that the Galois group $\mathrm{Gal}(F/K)$ of a finite Galois extension $F/K$ is isomorphic to a subgroup of $S_n$, where $n = [F : K]$. For example, by the primitive element theorem, $F = K(\alpha)$ for some $\alpha \in F$. Then $F$ is a splitting field of the minimal polynomial $f(x)$ of $\alpha$, and $\mathrm{Gal}(F/K)$ permutes $n$ roots of $f(x)$. This gives an embedding $\mathrm{Gal}(F/K) \hookrightarrow S_n$.

EXAMPLE 4.3.5. Let's completely analyze the field extension

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

We have an intermediate subfield $\mathbb{Q}(\sqrt{2})$ of degree 2 over $\mathbb{Q}$ and it is elementary to check that $\sqrt{3}$ is not contained in this subfield. It follows that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 4 over $\mathbb{Q}$ and is a splitting field of the polynomial $(x^2 - 2)(x^2 - 3)$. In particular, this extension is Galois. Let $G$ be the Galois group. Then

$$|G| = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

and $G$ permutes roots of $(x^2 - 2)(x^2 - 3)$. But not in an arbitrary way: $G$ can only permute roots of $x^2 - 2$ (resp. $x^2 - 3$). So we see that

$$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

It sends $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$. The group $G$ contains three proper subgroups: $H_1$ fixes $\sqrt{2}$, $H_2$ fixes $\sqrt{3}$, and $H_3$ can only change the sign of $\sqrt{2}$ and $\sqrt{3}$ simultaneously. Then $H_3$ fixes $\sqrt{6} = \sqrt{2}\sqrt{3}$. So there are 3 intermediate subfields: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{6})$.

Take an element $\sqrt{2}+\sqrt{3}$. Let $f(x)$ be its minimal polynomial. The Galois group $G$ permutes the roots of $f(x)$. So these roots must be $\pm\sqrt{2} \pm \sqrt{3}$. In particular, $f(x)$ has degree 4, and therefore $\sqrt{2} + \sqrt{3}$ is a primitive element:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

EXAMPLE 4.3.6. Whenever a group $G$ acts on a field $K$, we say that $K^G$ is the field of invariants of $G$. For example, consider the action of the symmetric group $S_n$ on the field of rational functions $K = k(x_1, \dots, x_n)$. By Lemma 4.3.2, $K/K^{S_n}$ is a Galois extension with a Galois group $S_n$. It is clear that $K^{S_n}$ contains elementary symmetric functions

$$\sigma_1 = \sum_i x_i, \quad \sigma_2 = \sum_{i<j} x_i x_j, \quad \dots, \quad \sigma_n = \prod_i x_i.$$

So $K^G \supset k(\sigma_1, \dots, \sigma_n)$. By the Vieta theorem, $k(x_1, \dots, x_n)$ is a splitting field over $k(\sigma_1, \dots, \sigma_n)$ of the polynomial

$$(x - x_1) \dots (x - x_n) = x^n - \sigma_1 x^{n-1} + \dots + (-1)^n \sigma_n$$

without multiple roots. It follows that $k(x_1, \dots, x_n)/k(\sigma_1, \dots, \sigma_n)$ is a Galois extension. Let $G$ be its Galois group. Since $G$ acts faithfully on the set of roots of the polynomial above, we have $|G| < n!$. Therefore, $K^G = k(\sigma_1, \dots, \sigma_n)$.

§4.4. **Exercises.**

In this set we fix a finite field extension $K \subset F$. Let $\bar{K}$ be an algebraic closure of $K$.

**1.** Let $\alpha \in F$ and let $f(x)$ be its minimal polynomial. Suppose that $\alpha$ is not separable over $K$. (a) Show that $\operatorname{char} K = p$ and $f(x) = g(x^p)$ for some polynomial $g \in K[x]$. (b) Show that there exists $k \geq 1$ such that all roots of $f(x)$ in $\bar{K}$ have multiplicity $p^k$ and $\alpha^{p^k}$ is separable over $K$.

**2.** (a) Show that elements of $F$ separable over $K$ form a field $L$. We define

$$[F : K]_s := [L : K].$$

(b) Prove that the number of different inclusions of $F$ in the algebraic closure of $K$ over $K$ is equal to $[F : K]_s$.

**3.** Show that $[F : K]_s = 1$ if and only if $\operatorname{char} K = p$ and $F$ is generated over $K$ by elements $\alpha_1, \dots, \alpha_r$ such that the minimal polynomial of each $\alpha_i$ has the form $x^{p^{k_i}} - a_i$ for some $a_i \in K$ and a positive integer $k_i$.

**4.** Show that the primitive element theorem does not necessarily hold for finite extensions that are not separable.

**5.** A field $k$ is called perfect if either $\operatorname{char} k = 0$ or $\operatorname{char} k = p$ and the Frobenius homomorphism $F : k \to k$ is an isomorphism. Show that if $k$ is perfect then any algebraic extension of $k$ is separable over $k$ and perfect.

**6.** Let $ABC$ be an isosceles triangle with $AB = BC$. Let $AD$ be a bisector of the angle $BAC$. Suppose that (a) $AD + BD = AC$ or (b) $BD = AC$. Find

the angle measure of the angle $BAC$ in degrees. (Hint: You can either use high school geometry (but the solution will be tricky) or algebra, in which case the Law of Sines could be helpful.)

**7.** Let $F$ be a splitting field of the polynomial $f \in K[x]$ of degree $n$. Show that $[F : K]$ divides $n!$ (do not assume that $F$ is separable over $K$).

**8.** Show that any element in a finite field is a sum of two squares in that field.

**9.** Let $F \subset \bar{K}$ be a finite Galois extension of $K$ and let $L \subset \bar{K}$ be any finite extension of $K$. Consider the natural $K$-linear map $L \otimes_K F \to \bar{K}$. (a) Show that its image is a field, that we will denote by $LF$. (b) Show that $LF$ is Galois over $L$. (c) Show that $\mathrm{Gal}(LF/L)$ is isomorphic to $\mathrm{Gal}(F/L \cap F)$.

**10.** Find the minimal polynomial over $\mathbb{Q}$ of $\sqrt[2]{3} + \sqrt[3]{3}$. Compute the Galois group of its splitting field.

**11.** Let $a, b \in K$ and suppose that $f(x) = x^3 + ax + b$ has no roots in $K$. Let $F$ be a splitting field of $f(x)$. Assume that $\mathrm{char}\, K \neq 3$. Show that

$$\mathrm{Gal}(F/K) \simeq \begin{cases} S_3 & \text{if } -4a^3 - 27b^2 \text{ is not a square in } K \\ \mathbb{Z}_3 & \text{if } -4a^3 - 27b^2 \text{ is a square in } K \end{cases}$$

**12.** Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree $p$. Suppose that $f(x)$ has exactly $p - 2$ real roots. Show that the Galois group of the splitting field of $f(x)$ is $S_p$.

**13.** For any $d \geq 2$, prove existence of an irreducible polynomial in $\mathbb{Q}[x]$ of degree $d$ with exactly $d - 2$ real roots (Hint: take some obvious reducible polynomial with exactly $d-2$ real roots and perturb it a little bit to make it irreducible).

**14.** Let $G$ be any finite group. Show that there exist finite extensions $\mathbb{Q} \subset K \subset F$ such that $F/K$ is a Galois extension with a Galois group $G$.

**15.** Let $F$ be a splitting field of the polynomial $f(x) \in K[x]$. Show that $\mathrm{Gal}\, F/K$ acts transitively on roots of $f(x)$ if and only if $f(x)$ is irreducible (do not assume that $f(x)$ is separable).

**16.** Let $F$ be a splitting field of a biquadratic polynomial $x^4 + ax^2 + b \in K[x]$. Show that $\mathrm{Gal}(F/K)$ is isomorphic to a subgroup of $D_4$.

## §5. Applications of Galois Theory - I

### §5.1. **Fundamental Theorem of Algebra.**

THEOREM 5.1.1. $\mathbb{C}$ *is algebraically closed.*

*Proof.* Since we are in $\mathrm{char} = 0$, all field extensions are separable. It suffices to show that any finite Galois extension $K$ of $\mathbb{R}$ is equal to $\mathbb{R}$ or to $\mathbb{C}$ (why?). We argue by induction on $[K : \mathbb{R}]$. If $[K : \mathbb{R}] = 1$ then $K = \mathbb{R}$ and there is nothing to prove. Suppose that $[K : \mathbb{R}] > 1$.

Let $G$ be a Galois group of $K/\mathbb{R}$. Let $H \subset G$ be its 2-Sylow subgroup. Then $[K^H : \mathbb{R}] = [G : H]$ is odd. Let $\alpha \in K^H$. Then the minimal polynomial of $\alpha$ in $\mathbb{R}[x]$ has odd degree. But any odd degree polynomial in $\mathbb{R}[x]$ has a root (this is the only place where we use analysis). Therefore $K^H = \mathbb{R}$, i.e. $G = H$ is a 2-group.

Any $p$-group has a non-trivial center. Let $\Gamma \subset Z(G)$ be a subgroup of order 2. Then $\Gamma$ is normal in $G$. Therefore, $K^\Gamma/\mathbb{R}$ is Galois. By inductive assumption, $K^\Gamma$ is equal to $\mathbb{R}$ or to $\mathbb{C}$.

Finally, $K/K^\Gamma$ is a quadratic extension. By the quadratic formula, any quadratic polynomial in $\mathbb{C}[x]$ splits and any quadratic polynomial in $\mathbb{R}[x]$ has a complex root. Therefore, $K^\Gamma = \mathbb{R}$ and $K = \mathbb{C}$. □

## §5.2. **Galois group of a finite field.**

THEOREM 5.2.1. *The Galois group* $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}_n$. *It is generated by the Frobenius map* $F(x) = x^p$. *Intermediate subfields* $\mathbb{F}_p \subset L \subset \mathbb{F}_{p^n}$ *correspond to divisors* $k$ *of* $n$. *We have* $L \simeq \mathbb{F}_{p^k}$ *and* $L = (\mathbb{F}_{p^n})^{F^k} = \{\alpha \in \mathbb{F}_{p^n} \mid \alpha^{p^k} = \alpha\}$.

*Proof.* Since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, the Galois group $G$ has order $n$. $G$ contains $F$. If $F$ has order $d$ then $\alpha^{p^d} = \alpha$ for any $\alpha \in \mathbb{F}_{p^n}$. A polynomial can not have more roots than its degree, therefore $d = n$ and $G \simeq \mathbb{Z}_n$. Notice that subgroups $H \subset G$ correspond to divisors $k|n$. Namely, $H$ is generated by $F^k$. The remaining statements follow from the main theorem of Galois theory. □

## §5.3. **Cyclotomic fields.**

Let $\phi(n) = |\mathbb{Z}_n^*|$ be the *Euler function*, i.e. the number of elements in $\mathbb{Z}_n$ coprime to $n$.

PROPOSITION 5.3.1. *Suppose* $n$ *is coprime to* $\operatorname{char} k$. *Let* $K/k$ *be the splitting field of* $x^n - 1$ *(in which case we say that* $K$ *is obtained from* $k$ *by adjoining* $n$*-th roots of unity). Then* $[K : k]$ *divides* $\phi(n)$ *and* $\mathrm{Gal}(K/k)$ *is isomorphic to a subgroup of* $(\mathbb{Z}/n\mathbb{Z})^*$

*Proof.* Let $\mu_n \subset K$ be the solutions of $x^n - 1 = 0$. Notice that $\mu_n$ is cyclic (as any finite subgroup in the multiplicative group of a field) and has order $n$ (because $x^n - 1$ is separable). Let $G = \mathrm{Gal}(K/k)$. Notice that $G$ acts faithfully on $\mu_n$ by automorphisms. So $G$ is isomorphic to a subgroup of $\mathrm{Aut}(\mu_n)$, which has $\phi(n)$ elements. So $|G|$ divides $\phi(n)$. □

DEFINITION 5.3.2. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Since any $n$-th root of 1 is a power of $\zeta_n$, the splitting field of $x^n - 1$ is equal to $\mathbb{Q}(\zeta_n)$. This field is called the *cyclotomic field* (Etymology: cyclotomy is the process of dividing the circle into equal parts, from cycl- + -tomy).

THEOREM 5.3.3. *Let* $\zeta = \zeta_n$. *The cyclotomic field* $\mathbb{Q}(\zeta)$ *has degree* $\phi(n)$ *over* $\mathbb{Q}$. *The Galois group of* $\mathbb{Q}(\zeta)/\mathbb{Q}$ *is equal to* $\mathbb{Z}_n^*$. *The minimal polynomial of* $\zeta$ *is*

$$\Phi_n(x) = \prod_{\substack{0<k<n \\ (k,n)=1}} (x - \zeta^k)$$

*(the cyclotomic polynomial). We have* $x^n - 1 = \prod_{d|n} \Phi_d$.

*Proof.* Let $f(x)$ be the minimal polynomial of $\zeta$. We already know that $\deg f$ divides $\phi(n)$ and that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a subgroup of $\mathbb{Z}_n^*$. We claim that $f(\zeta^k) = 0$ whenever $(k, n) = 1$. This will show that $f(x) = \Phi_n(x)$, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$, and $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathbb{Z}_n^*$.

Arguing by induction on $k$, it suffices to show that $f(\zeta^p) = 0$ if $p$ is prime and does not divide $n$. Arguing by contradiction, suppose that $f(\zeta^p) \neq 0$. Let

$$x^n - 1 = f(x)g(x).$$

Then $g(\zeta^p) = 0$. It follows that $\zeta$ is a root of $g(x^p)$. Therefore, we have

$$g(x^p) = f(x)h(x). \tag{10}$$

By Gauss lemma, polynomials $f(x)$, $g(x)$, and $g(x)$ have integer coefficients (and are monic). So we can reduce (10) modulo $p$:

$$g(x)^p \equiv g(x^p) \equiv f(x)h(x) \mod p$$

Let $\bar{f}(x)$ and $\bar{g}(x)$ be polynomials in $\mathbb{Z}_p[x]$ obtained by reducing $f(x)$ and $g(x)$ modulo $p$. Then $\bar{f}(x)$ divides $\bar{g}(x)^p$, and therefore $\bar{f}(x)$ and $\bar{g}(x)$ are not coprime. Therefore, $x^n - 1 = \bar{f}(x)\bar{g}(x)$ has a multiple root in some finite field containing $\mathbb{F}_p$. But since $(p, n) = 1$, $(nx^{n-1}, x^n - 1) = 1$, and therefore $x^n - 1$ has no multiple roots. □

§5.4. **Kronecker–Weber Theorem.** The role played by cyclotomic fields can be appreciated for the following theorem (proved by Kronecker and Weber)

THEOREM 5.4.1. *Any Galois extension $K/\mathbb{Q}$ with an Abelian Galois group is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$.*

This remarkable theorem is very difficult, and attempts to generalize it to Abelian extensions of fields of algebraic numbers led to the development of Class Field Theory (and to modern Langlands program). Let's just prove the easiest case, first observed by Gauss:

THEOREM 5.4.2. *Any quadratic extension $K/\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$.*

*Proof.* Any quadratic extension of $\mathbb{Q}$ has the form $\mathbb{Q}(\sqrt{n})$, where $n$ is a square-free integer. Let $n = p_1 \dots p_r$ be a prime decomposition.

Notice that $\zeta_l \in \mathbb{Q}(\zeta_m)$ if $l|m$. It follows that if $\sqrt{p_i} \in \mathbb{Q}(\zeta_{l_i})$ for any $i$ then $\sqrt{n} \in \mathbb{Q}(\zeta_{l_1 \dots l_r})$. So it suffices to prove that $\sqrt{p}$ is contained in a cyclotomic field when $p$ is a prime.

The case $p = 2$ is easy ($\sqrt{2} = e^{\pi i/4} + e^{-\pi i/4}$). We assume that $p$ is odd.

For any $\nu \in \mathbb{F}_p^*$, let $(\frac{\nu}{p})$ be the *quadratic (or Legendre) symbol*. It is equal to $1$ if $\nu$ is a square in $\mathbb{F}_p$ and $-1$ otherwise. It is multiplicative (why?):

$$\left(\frac{\nu}{p}\right)\left(\frac{\nu'}{p}\right) = \left(\frac{\nu\nu'}{p}\right).$$

Let $\zeta = \zeta_p$ and consider the *Gauss sum*

$$S = \sum_{\nu \in \mathbb{F}_p^*} \left(\frac{\nu}{p}\right) \zeta^\nu.$$

We claim (after Gauss) that

$$S^2 = \left(\frac{-1}{p}\right) p$$

and therefore $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $(\frac{-1}{p}) = 1$ and $i\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $(\frac{-1}{p}) = -1$. In the latter case $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$ (because $i \in \mathbb{Q}(\zeta_4)$).

This is a fun calculation with a neat trick:

$$S^2 = \sum_{\nu,\mu\in\mathbb{F}_p^*} \left(\frac{\nu}{p}\right)\left(\frac{\mu}{p}\right)\zeta^{\nu+\mu} = \sum_{\nu,\mu\in\mathbb{F}_p^*} \left(\frac{\nu\mu}{p}\right)\zeta^{\nu+\mu} =$$

the trick is to replace $\nu$ with $\nu\nu$ for any fixed $\mu$, which gives

$$= \sum_{\nu,\mu\in\mathbb{F}_p^*} \left(\frac{\nu\mu^2}{p}\right)\zeta^{\nu\mu+\mu} = \sum_{\nu,\mu\in\mathbb{F}_p^*} \left(\frac{\nu}{p}\right)\zeta^{\mu(\nu+1)} =$$

$$\sum_{\mu\in\mathbb{F}_p^*} \left(\frac{-1}{p}\right)\zeta^0 + \sum_{\nu\neq -1} \left(\frac{\nu}{p}\right) \sum_{\mu\in\mathbb{F}_p^*} \zeta^{\mu(\nu+1)} =$$

It is easy to see that $\sum_{\mu\in\mathbb{F}_p}(\zeta^{\nu+1})^\mu = 0$ (why?)

$$= \left(\frac{-1}{p}\right)(p-1) - \sum_{\nu\neq -1}\left(\frac{\nu}{p}\right) = p\left(\frac{-1}{p}\right),$$

because $\sum\limits_{\nu\in\mathbb{F}_p}\left(\frac{\nu}{p}\right) = 0$ (why?) □

The most famous fact about quadratic symbols is the *reciprocity law*

THEOREM 5.4.3 (Gauss' *Theorema Aureum*).

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}},$$

*where $p$ and $q$ are odd primes.*

*Proof.* It is straightforward to check (see Exercise 2) that

$$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \mod q.$$

In the previous proof we have obtained the identity

$$S^2 = p\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}p,$$

where $S$ is the Gauss sum (see Exercise 2 for the last equality). So we have

$$S^{q-1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \mod q,$$

where we work in the ring $\mathbb{Z}[\zeta_p]$. So "$a \equiv b \mod q$" means "$a - b \in (q)$". On the other hand,

$$S^q \equiv \sum_{\nu\in\mathbb{F}_p^*}\left(\frac{\nu}{p}\right)^q\zeta^{\nu q} \qquad \text{(Frobenius!)}$$

$$\equiv \sum_{\nu\in\mathbb{F}_p^*}\left(\frac{\nu}{p}\right)\zeta^{\nu q} \equiv \sum_{\nu\in\mathbb{F}_p^*}\left(\frac{\nu q}{p}\right)\left(\frac{q}{p}\right)\zeta^{\nu q} \equiv$$

$$\equiv \left(\frac{q}{p}\right)S \mod q.$$

We can combine two formulas for $S^q$ to get the quadratic reciprocity law, but we have to be slightly careful because we are doing calculations in $\mathbb{Z}[\zeta_p]$ rather than in $\mathbb{Z}$. We can finish as follows. We have proved that

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)S \equiv \left(\frac{q}{p}\right)S \mod q$$

This implies

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)S^2 \equiv \left(\frac{q}{p}\right)S^2 \mod q.$$

But $S^2 = \pm p$, so this congruence is a congruence in $\mathbb{Z}$, and since $(p,q)=1$, we can cancel $S^2$. This finally gives

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

QED □

§5.5. **Cyclic Extensions.** As we know, any quadratic extension $F/K$ can be obtained by simply adding a quadratic root (of the discriminant) $F = K(\sqrt{D})$. It turns out that a very similar description is available for any Galois extension with a cyclic Galois group:

THEOREM 5.5.1. *Suppose that $K$ contains all $n$-th roots of $1$ and that $\operatorname{char} K$ does not divide $n$.*

- *Let $\alpha$ be a root of $x^n - a$ for some $a \in K$. Then $K(\alpha)/K$ is Galois, and the Galois group is cyclic of order $d$, where $d|n$ and $\alpha^d \in K$.*
- *If $F/K$ is a Galois extension with a cyclic Galois group of order $n$ then $F = K(\alpha)$ for some $\alpha \in F$ such that $\alpha^n \in K$.*

*Proof.* Let $\zeta \in K$ be a primitive $n$-th root of $1$.

One direction is easy: Let $\alpha$ be a root of $x^n - a$ for some $a \in K$. Then $\zeta^k\alpha$ is also a root for any $1 \le k \le n-1$. It follows that $x^n - a$ splits in $K(\alpha)$. Since all the roots are distinct, we see that $K(\alpha)/K$ is Galois. Let $G$ be the Galois group. For any $g \in G$, we have $g\alpha = \zeta^k\alpha$ for some $k \in \mathbb{Z}/n\mathbb{Z}$. It is easy to see that this gives an injective homomorphism

$$G \to \mathbb{Z}/n\mathbb{Z}, \quad g \mapsto k$$

Therefore, $G$ is cyclic of order $d|n$. Let $\sigma$ be a generator. Then $\sigma(\alpha) = \nu\alpha$, where $\nu^d = 1$. We have

$$\sigma(\alpha^d) = [\sigma(\alpha)]^d = \nu^d\alpha^d = \alpha^d.$$

It follows that $\alpha^d \in K$.

Now a less trivial implication: Let $F/K$ be a Galois extension with a cyclic Galois group $G$ of order $n$. Let $\sigma$ be a generator of the Galois group. It suffices to prove the following:

CLAIM 5.5.2. *There exists $\alpha \in F^*$ such that $\sigma(\alpha) = \zeta\alpha$.*

Indeed, given the Claim, and since the Galois group acts transitively on roots of the minimal polynomial of $\alpha$, we see that the minimal polynomial of $\alpha$ is equal to

$$f(x) = (x-\alpha)(x-\zeta\alpha)\dots(x-\zeta^{n-1}\alpha).$$

In particular, $[K(\alpha):K]=n$, and therefore $K(\alpha)=F$. Finally,

$$\sigma(\alpha^n)=\zeta^n\alpha^n=\alpha^n,$$

and therefore $\alpha^n=a\in K$ (it also follows that $f(x)=x^n-a$).

Next we prove the Claim. Since $\sigma^n=\mathrm{Id}$, the minimal polynomial of $\sigma$ (as a $K$-linear operator) divides $\lambda^n-1$. It follows that all eigenvalues of $\sigma$ are $n$-th roots of unity. Since

$$F^\sigma=\{\alpha\in F\,|\,\sigma(\alpha)=\alpha\}=K$$

by the main theorem of Galois Theory, $\sigma$ has an eigenvector $\alpha$ with an eigenvalue $\lambda\neq 1$, $\lambda^n=1$. If $n$ is prime, $\lambda$ is automatically a primitive $n$-th root of unity, and we can stop here. But if $n$ is not prime, $\lambda$ is not necessarily primitive, this argument needs a further analysis.

We will give another proof, which utilizes a useful formula discovered by Lagrange. It is now called a *Lagrange resolvent*.

Consider the following $K$-linear operator on $F$:

$$A=\mathrm{Id}+\zeta^{-1}\sigma+\ldots+\zeta^{-(n-1)}\sigma^{n-1}.$$

By Lemma 5.5.3 below, this operator is not identically $0$. Let $\beta\in F$ be any element such that $\alpha:=A(\beta)\neq 0$. Then

$$\alpha=\beta+\zeta^{-1}\sigma(\beta)+\ldots+\zeta^{-(n-2)}\sigma^{n-2}(\beta)+\zeta^{-(n-1)}\sigma^{n-1}(\beta) \tag{11}$$

and

$$\sigma(\alpha)=\sigma(\beta)+\zeta^{-1}\sigma^2(\beta)+\ldots+\zeta^{-(n-2)}\sigma^{n-1}(\beta)+\zeta^{-(n-1)}\sigma^n(\beta)=$$

$$=\zeta\beta+\sigma(\beta)+\zeta^{-1}\sigma^2(\beta)+\ldots+\zeta^{-(n-2)}\sigma^{n-1}(\beta)=\zeta\alpha.$$

We are done! □

LEMMA 5.5.3 (Artin). *Let $F$ be a field and let $\sigma_1,\ldots,\sigma_r$ be different automorphisms of $F$. Then they are linearly independent over $K$: if $\alpha_1\sigma_1+\ldots+\alpha_r\sigma_r=0$ as a $K$-linear operator $F\to F$ for some $\alpha_1,\ldots,\alpha_r\in F$ then $\alpha_1=\ldots=\alpha_r=0$.*

*In fact, more is true: let $F$ be a field, let $\Gamma$ be a group, and let $\sigma_i:\Gamma\to F^*$ for $i\in I$ be different homomorphisms (so called characters). Then they are linearly independent over $K$: if $\alpha_1\sigma_1+\ldots+\alpha_r\sigma_r=0$ as a function $\Gamma\to F$ for some $\alpha_1,\ldots,\alpha_r\in F$ then $\alpha_1=\ldots=\alpha_r=0$.*

*Proof.* The first part follows from the second: just take $\Gamma=F^*$ (any automorphism obviously induces a multiplicative homomorphism $F^*\to F^*$).

To prove the second part, suppose we have a relation

$$\alpha_1\sigma_1+\ldots+\alpha_r\sigma_r=0.$$

We can assume that $r$ is the minimal possible. Then $r\geq 2$ and $\alpha_i\neq 0$ for any $i$. Since $\sigma_1,\sigma_2$ are different, there exists $z\in\Gamma$ such that $\sigma_1(z)\neq\sigma_2(z)$. Then we have

$$\alpha_1\sigma_1(xz)+\ldots+\alpha_r\sigma_r(xz)=0$$

for any $x\in G$, and therefore

$$\alpha_1\sigma_1(z)\sigma_1+\ldots+\alpha_r\sigma_r(z)\sigma_r=0$$

is *another* linear relation on our homomorphisms. Divide by $\sigma_1(z)$, and subtract from the first relation. This gives

$$\left(\alpha_2\frac{\sigma_2(z)}{\sigma_1(z)}-\alpha_2\right)\sigma_2+\ldots=0.$$

This is a non-trivial relation of a smaller length, a contradiction. □

§5.6. **Composition Series and Solvable Groups.** We would like to understand Galois extensions with solvable Galois groups (which was the main contribution of Galois to Galois theory). Let us use this opportunity and make a digression into group theory and discuss composition series. These results are very general and the arguments rely only on the first and the second isomorphism theorem. So they hold not just for groups but also for $R$-modules, Lie algebras, etc.

DEFINITION 5.6.1. A group $G$ is called *simple* if it is not trivial, and has no normal subgroups other than $\{e\}$ and $G$ itself.

EXAMPLE 5.6.2. $\mathbb{Z}/p\mathbb{Z}$ for prime $p$, $A_n$ for $n\geq 5$.

DEFINITION 5.6.3. Let $G$ be a group. A sequence of subgroups

$$G=G_1\supset G_2\supset G_3\supset\ldots\supset G_r=\{e\} \tag{5}$$

is called a *tower* (or a *series* or a *filtration*). A *refinement* of (5) is a tower obtained by inserting a finite number of subgroups in the given tower.

The tower is called *normal* if each $G_{i+1}$ is normal in $G_i$. A normal tower (5) is called *composition series* if each quotient $G_i/G_{i+1}$ (called *composition factor*) is a simple group.

The tower is called *Abelian* (resp. *cyclic*) if it is normal and each quotient $G_i/G_{i+1}$ is Abelian (resp. cyclic).

A group $G$ is called *solvable* if it has an Abelian tower.

Here are some simple facts:

LEMMA 5.6.4. *A normal tower of a finite group can be refined to composition series. An Abelian tower* (5) *of a finite solvable group can be refined to a cyclic tower such that its subsequent quotients are simple cyclic groups $\mathbb{Z}/p\mathbb{Z}$ (for various prime $p$).*

*Proof.* Take a normal tower (5) of $G$ and assume that this tower is Abelian if $G$ is solvable. If one of the quotients $G_i/G_{i+1}$ is not simple (i.e. is not isomorphic to $\mathbb{Z}/p\mathbb{Z}$ in the solvable case) then let $H\subset G_i/G_{i+1}$ be a proper normal subgroup. We refine the tower as follows:

$$G_i\supset p^{-1}(H)\supset G_{i+1},$$

where $p: G_i\to G_i/G_{i+1}$ is the quotient map. This refinement procedure must stop after at most $\log_2|G|$ steps. □

LEMMA 5.6.5. *Any finite $p$-group $G$ is solvable.*

*Proof.* Induction on $G$. A basic fact about finite $p$-groups is that their center $Z(G)$ is not-trivial. We have a normal tower

$$G\supset Z(G)\supset\{e\}.$$

The quotient group $G/Z(G)$ is a $p$-group of smaller size, so by induction it has an Abelian tower. Pulling back this tower to $G$ gives an Abelian refinement of the inclusion $G \supset Z(G)$. □

LEMMA 5.6.6. *A subgroup $H$ of a solvable group $G$ is solvable.*

*Proof.* Take an Abelian tower of (5). It induces the tower

$$H = H_1 = H \cap G_1 \supset H_2 = H \cap G_2 \supset \ldots \supset H_r = H \cap G_r.$$

Since $G_{i+1}$ is normal in $G_i$, $H_{i+1} = G_{i+1} \cap H$ is normal in $H_i = G_i \cap H$. The inclusion $H_i \subset G_i$ induces the inclusion $H_i/H_{i+1} \subset G_i/G_{i+1}$. Therefore $H_i/H_{i+1}$ is Abelian. □

DEFINITION 5.6.7. Two normal towers of the same group, say (5) and

$$G = H_1 \supset H_2 \supset H_3 \supset \ldots \supset H_s = \{e\} \tag{6}$$

are called *equivalent* if $r = s$ and the sequence of consequent quotients

$$G_1/G_2,\ G_2/G_3,\ \ldots,\ G_{r-1}/G_r = G_{r-1}$$

can be rearranged so that they are respectively isomorphic to

$$H_1/H_2,\ H_2/H_3,\ \ldots,\ H_{s-1}/H_s = H_{s-1}.$$

Here is a first surpise: a very useful theorem of Jordan and Hölder.

THEOREM 5.6.8. *Any two composition series of a group $G$ are equivalent.*

Since the composition series is a tower that cannot be refined, the Jordan–Hölder theorem obviously follows from the following even more general theorem of Schreier:

THEOREM 5.6.9. *Any two normal towers of $G$ have equivalent refinements.*

*Proof.* Let the two towers (5) and (6) be given. For each $i = 1, \ldots, r-1$ and $j = 1, \ldots, s$ we define

$$G_{ij} = G_{i+1}(H_j \cap G_i).$$

Notice that since $G_{i+1}$ is normal in $G_i$, $G_{ij}$ is a subgroup of $G_i$ and we can refine our tower by inserting blocks

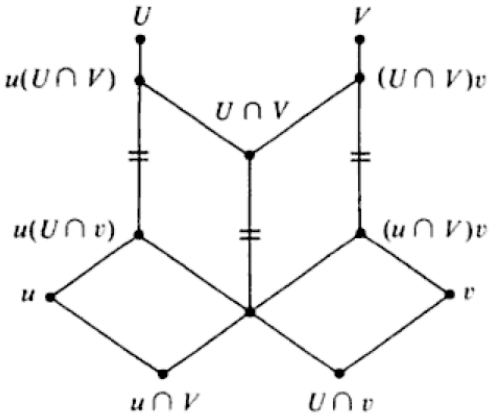
$$G_i = G_{i1} \supset G_{i2} \supset \ldots \supset G_{is} = G_{i+1}.$$

Similarly, we can define

$$H_{ji} = H_{j+1}(G_i \cap H_j)$$

for $j = 1, \ldots, s-1$ and $i = 1, \ldots, r$. This gives a refinement of the first tower. Both refined towers have $(r-1)(s-1)+1$ elements, namely $G_{ij}$ and $\{e\}$ in the first case and $H_{ji}$ and $\{e\}$ in the second case, where the range for indices is $i = 1, \ldots, r-1$, $j = 1, \ldots, s-1$. We claim that these two towers are equivalent, and more precisely, the quotients of $G_{ij}$ and $H_{ji}$ are isomorphic. This is the content of the next lemma. □

LEMMA 5.6.10 (Zassenhaus Lemma, or Butterfly Lemma). *Let $U, V$ be subgroups of a group $G$. Let $u, v$ be normal subgroups of $U$, $V$, respectively. Then $u(U \cap v)$ is normal in $u(U \cap V)$, $(u \cap V)v$ is normal in $(U \cap V)v$, and the quotient groups are isomorphic.*




*Proof.* Subgroups appearing in the proof form a butterfly (reproduced from Lang's Algebra). We are not going to use this in the proof, but playing with this diagram will convince you that whenever two groups are connected by a segment to a point lying right above, this point represents their product, and whenever the point lies right below, it represents their intersection.

The main claim is that quotient groups formed along the three central vertical lines are all isomorphic.

Since $U \cap V$ normalizes $u$, we see that $u(U \cap V)$ is a subgroup.

Set $H = U \cap V$ and $N = u(U \cap v)$. Then $H$ normalizes $N$ and by the second isomorphism theorem for groups we have

$$HN/N \simeq H/H \cap N.$$

A small calculation shows that

$$H \cap N = U \cap V \cap \big(u(U \cap v)\big) = (u \cap V)(U \cap v)$$

and

$$HN = (U \cap V)u(U \cap v) = (U \cap V)u = u(U \cap V).$$

This gives

$$\big(u(U \cap V)\big)/\big(u(U \cap v)\big) \simeq (U \cap V)/\big((u \cap V)(U \cap v)\big).$$

The lemma follows from symmetry between $U$ and $V$. □

§5.7. **Exercises.**

**1.** Let $p_1, \dots, p_r \in \mathbb{Z}$ be distinct primes and let $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})$. (a) Compute the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. (b) Describe explicitly all intermediate subfields $L$ such that either $[L : \mathbb{Q}] = 2$ or $[K : L] = 2$. (c) Describe explicitly all intermediate subfields when $r = 4$.

**2.** Let $q$ be an odd prime and let $a$ be an integer coprime to $q$. Show that the quadratic symbol $(\frac{a}{q})$ is equal to $a^{\frac{q-1}{2}}$ modulo $q$.

**3.** Consider a tower $K \subset L \subset F$. Suppose $L/K$ and $F/L$ are finite Galois extensions. Is it true that $F/K$ is Galois?

**4.** Let $\alpha_r = \sqrt{2 + \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2}}}}$ ($r$ radicals). (a) Show that the minimal polynomial $f_r(x) \in \mathbb{Q}[x]$ of $\alpha_r$ can be computed inductively as follows:

$f_r(x) = f_{r-1}(x^2-2)$, where $f_1(x) = x^2-2$. Describe all roots of $f_r(x)$. (b) Show that $\mathbb{Q}(\alpha_2)/\mathbb{Q}$ is a Galois extension with a Galois group $\mathbb{Z}_4$.

**5.** Let $K \subset L \subset \bar{K}$ and suppose that $L/K$ is separable. Show that there exists the unique minimal (by inclusion) Galois extension $F/K$ such that $L \subset F \subset \bar{K}$. Show that if $L/K$ is finite then $F/K$ is finite.

**6.** (a) Let $\bar{K}$ be an algebraic closure of $K$. Show that there exists the unique maximal (by inclusion) subfield $K \subset K^{ab} \subset \bar{K}$ such that $K^{ab}/K$ is Galois and the Galois group $\mathrm{Gal}(K^{ab}/K)$ is Abelian. (b) Deduce from the Kronecker-Weber Theorem that

$$\mathbb{Q}^{ab} = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n).$$

**7.** Let $F/K$ be a finite Galois extension with a Galois group $G$. Let $H \subset G$ be a subgroup and let $L = F^H$. Show that the number of fields of the form $g(L)$ for $g \in G$ is equal to $\frac{|G|}{|N_G(H)|}$.

**8.** Let $F/K$ be a finite Galois extension with a Galois group $G$. Let $H \subset G$ be a subgroup and let $L = F^H$. Let $N = \bigcap\limits_{g\in G} gHg^{-1}$. Prove that $N$ is normal in $G$ and characterize the field $F^N$ in terms of the tower $K \subset L \subset F$.

**9.** Let $F/K$ be a splitting field of a polynomial $f(x) = (x-a_i)\dots(x-a_r) \in K[x]$ without multiple roots. Let

$$\Delta = \prod_{1\leq i<j\leq n} (a_i - a_j)^2$$

be the discriminant of $f(x)$. (a) Show that $\Delta \in K$. (b) Let $G \subset S_n$ be the Galois group of $F/K$ acting on roots of $f(x)$. Show that $G \subset A_n$ if and only if $\Delta$ is a square in $K$.

**10.** Let $F = \mathbb{C}(x_1, \dots, x_n)$ be the field of rational functions in $n$ variables. (a) Suppose $A_n$ acts on $F$ by even permutations of variables. Show that $F^{A_n}$ is generated over $\mathbb{C}$ by elementary symmetric functions $\sigma_1, \dots, \sigma_n$ in variables $x_1, \dots, x_n$ and by $\prod\limits_{1\leq i<j\leq n} (x_i - x_j)$. (b) Suppose $n = 4$ and suppose $D_4$ acts on $F$ by permutations of variables (here we identify variables with vertices of the square). Show that $F^{D_4}$ is generated over $\mathbb{C}$ by $4$ functions and find them.

**11.** Let $G$ be a finite Abelian group. (a) Show that there exists a positive integer $n$ and a subgroup $\Gamma \subset \mathbb{Z}_n^*$ such that $G \simeq \mathbb{Z}_n^*/\Gamma$. (b) Show that there exists a Galois extension $K/\mathbb{Q}$ with a Galois group $G$. (It is a famous open problem to remove an Abelian assumption from this exercise).

**12.** Compute the Galois group of the polynomial (a) $x^3 - x - 1$ over $\mathbb{Q}(\sqrt{-23})$; (b) $x^3 - 2tx + t$ over $\mathbb{C}(t)$ (the field of rational functions in one variable).

**13.** Compute the Galois group of the polynomial $x^4 - 4x^2 - 1$ over $\mathbb{Q}$.

**14.** Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial such that one of its complex roots has absolute value $1$. Show that $f(x)$ has even degree and is palindromic: if $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ then $a_0 = a_n$, $a_1 = a_{n-1}$, etc.

**15.** Let $\Phi_n(x)$ be the $n$-th cyclotomic polynomial, $a$ a non-zero integer, $p$ a prime. Assume that $p$ does not divide $n$. Prove that $p|\Phi_n(a)$ if and only if $a$ has order $n$ in $(\mathbb{Z}/p\mathbb{Z})^*$.

**16.** Let $K = \mathbb{C}[z^{-1}, z]]$ be the field of Laurent series (series in $z$, polynomials in $z^{-1}$). Let $K_m = \mathbb{C}[z^{\frac{-1}{m}}, z^{\frac{1}{m}}]] \supset K$. (a) Show that $K_m/K$ is Galois with a Galois group $\mathbb{Z}/m\mathbb{Z}$. (b) Show that any Galois extension $F/K$ with a Galois group $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to $K_m$. (c) In the notation of Problem 6, show that

$$K^{ab} = \bigcup_{m\geq 1} K_m,$$

the field of Puiseux series[2].

**17.** Show that any group of order $n$ is solvable, where (a) $n = p^2q$ and $p, q$ are distinct primes; (b) $n = 2pq$ and $p, q$ are odd primes.

**18.** Let $M$ be a module over a ring $R$. A sequence of submodules

$$M = M_1 \supset M_2 \supset \ldots \supset M_r = 0$$

is called a filtration of $M$ (of length $r$). A module $M$ is called simple if it does not contain any submodules other than $0$ and itself. A filtration is called simple if each $M_i/M_{i+1}$ is simple. A module $M$ is said to be of finite length if it admits a simple finite filtration. Two filtrations of $M$ are called equivalent if they have the same length and the same collection of subquotients $\{M_1/M_2, M_2/M_3, \ldots, M_{r-1}/M_r\}$ (up to isomorphism). Prove that if $M$ has finite length then any two simple filtrations of $M$ are equivalent and any filtration of $M$ can be refined to a simple filtration.

**19.** Describe all Abelian groups $G$ that fit into the exact sequence

$$0 \to \mathbb{Z}_n \to G \to \mathbb{Z}_m \to 0$$

($n$ and $m$ are not necessarily coprime).

## §6. Applications of Galois Theory -II

§6.1. **Solvable extensions: Galois Theorem.** In this section we will assume for simplicity that

$$\operatorname{char} K = 0.$$

Alternatively, one can assume that all extensions we consider are separable and their degrees are not divisible by characteristic.

Definition 6.1.1.

- A finite extension $F/K$ is called *solvable* if there exists a Galois extension $L/K$ containing $F$ with a solvable Galois group.
- A finite extension $F/K$ is called *solvable by radicals* if there exists a finite extension $L/K$ containing $F$ and admitting a tower

  $$K = L_0 \subset L_1 \subset \ldots \subset L_r = L$$

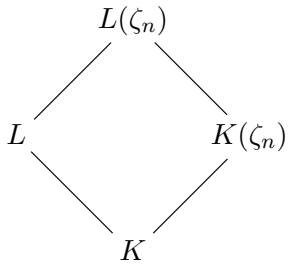
  such that on each step $L_i = L_{i-1}(\alpha)$, where $\alpha^n \in L_{i-1}$ for some $n$.

Theorem 6.1.2. *$F/K$ is solvable if and only if it is solvable by radicals.*

[2]Newton proved that the field of Puiseux series is in fact algebraically closed.

*Proof.* All fields appearing in the proof will be subfields of the fixed algebraic closure $\bar{K}$. Let $F/K$ be a solvable extension. Let $L/K$ be the Galois extension containing $F$ with a solvable Galois group $G$ of size $n$.

Let $K(\zeta_n)$ be the splitting field of $x^n - 1$. Consider the diagram of fields




The extension $L(\zeta_n)/K(\zeta_n)$ is Galois. Its Galois group $H$ is isomorphic to a Galois group of $L/L \cap K(\zeta_n)$ (Problem 9 from the previous homework), which is a subgroup of $G$. Therefore, $H$ is solvable.

A cyclic tower of subgroups

$$H = H_1 \supset H_2 \supset \ldots \supset H_r = \{e\}$$

gives rise to a tower of subfields

$$K(\zeta_n) = J_1 \subset J_2 \subset \ldots \subset J_r = L(\zeta_n),$$

where

$$J_i = L(\zeta_n)^{H_i}.$$

By the main Theorem on Galois theory, $L(\zeta_n)/J_i$ is Galois with a Galois group $H_i$. Since $H_{i+1}$ is normal in $H_i$, $J_{i+1}/J_i$ is Galois with a Galois group $H_i/H_{i+1}$, which is cyclic.

Since $J_{i+1}/J_i$ is a cyclic extension of degree $d|n$ (by Lagrange Theorem), and $J_i$ contains $n$-th roots of unity, we can apply Theorem 5.5.1. We see that on each step $J_{i+1} = J_i(\alpha)$, where some power of $\alpha$ belongs to $J_{i-1}$, i.e. $F/K$ is solvable in radicals.

Conversely, suppose $F/K$ is solvable in radicals, i.e. $F$ is contained in a field $L$ that admits a tower

$$K \subset L_1 \subset \ldots \subset L_r = L$$

such that on each step $L_i = L_{i-1}(\alpha)$, where $\alpha^k \in L_{i-1}$ for some $k$. Let $n$ be the l.c.m. of $k$'s that appear. Consider the tower of fields

$$K \subset K(\zeta_n) \subset L_1(\zeta_n) \subset \ldots \subset L_r(\zeta_n) = M,$$

where each consecutive embedding is Galois with an Abelian Galois group on the first step (by Theorem 5.3.1) and a cyclic Galois group for the remaining steps (by Theorem 5.5.1). Let $g_1, \ldots, g_k : M \to \bar{K}$ be the list of all embeddings over $K$. Each of the embeddings $g(M) \subset \bar{K}$ has the same property as above: in the corresponding tower

$$K \subset g \cdot K(\zeta_n) \subset g \cdot L_1(\zeta_n) \subset \ldots \subset g \cdot M,$$

each consecutive embedding is Galois with an Abelian Galois group. We can combine the towers above to refine the tower

$$K \subset M = g_1(M) \subset g_1(M)g_2(M) \subset \ldots g_1(M) \ldots g_k(M)$$

to a tower that has the same property as above (by Problem 9 from the previous homework). The field extension $\mathcal{M} = g_1(M)\dots g_k(M)$ is clearly Galois (in fact this the minimal Galois extension that contains $M$). Its tower of subfields induces an Abelian tower of subgroups of $\mathrm{Gal}(\mathcal{M}/K)$. □

## §6.2. **Norm and Trace.**

DEFINITION 6.2.1. Let $F/K$ be a separable extension of degree $n$ and let $\sigma_1,\dots,\sigma_n : F \to \bar{K}$ be the set of all embeddings over $K$. Let $\alpha \in F$. We define its trace

$$\mathrm{Tr}_{F/K}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$$

and norm

$$N_{F/K}(\alpha) = \sigma_1(\alpha)\dots\sigma_n(\alpha).$$

EXAMPLE 6.2.2. We have $N_{\mathbb{C}/\mathbb{R}}(a+ib) = (a+ib)(a-ib) = a^2+b^2$.

One has to be careful: the norm and the trace depend on the extension and not just on $\alpha$. But this dependence is easy to understand:

LEMMA 6.2.3. *Let $F/K$ and $L/F$ be separable extensions and let $\alpha \in F$. Then*

$$\mathrm{Tr}_{L/K}(\alpha) = [L:F]\,\mathrm{Tr}_{F/K}(\alpha) \quad \text{and} \quad N_{L/K}(\alpha) = N_{F/K}(\alpha)^{[L:F]}.$$

*Proof.* This is clear: any embedding $L \to \bar{K}$ over $K$ is obtained by extending some embedding $\sigma : F \to \bar{K}$. There are $[L:F]$ possible extensions, and neither of them changes $\sigma(\alpha)$. □

As a consequence of Artin's Lemma 5.5.3, we see that

COROLLARY 6.2.4. *The trace $\mathrm{Tr}_{F/K}$ is not identically zero.*

There are two simple ways to compute the trace and the norm:

LEMMA 6.2.5. *Let $f(x) = x^k + a_1x^{k-1} + \dots + a_k$ be the minimal polynomial of $\alpha$. Then*

$$\mathrm{Tr}_{K(\alpha)/K}(\alpha) = -a_1 \quad \text{and} \quad N_{K(\alpha)/K}(\alpha) = (-1)^k a_k$$

*The trace is an additive homomorphism $\mathrm{Tr}_{F/K} : F \to K$. The norm is a multiplicative homomorphism $N_{F/K} : F^* \to K^*$.*

*Proof.* Notice that embeddings $K(\alpha) \to \bar{K}$ just send $\alpha$ to various roots of $f(x)$. So the lemma follows from Vieta formulas. □

Here is another way to compute the norm and the trace:

LEMMA 6.2.6. *Let $\alpha \in F$ and let $A$ be a $K$-linear operator $F \to F$ of left multiplication by $\alpha$. Then $\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}(A)$ and $N_{F/K}(\alpha) = \det(A)$.*

*Proof.* Let $e_1,\dots,e_r$ be a basis of $F$ over $K(\alpha)$. Then as a $K$-vector space, $F$ is a direct sum of vector subspaces

$$F = K(\alpha)e_1 \oplus \dots \oplus K(\alpha)e_r.$$

Choosing a basis of $F$ compatible with this decomposition, we see that the matrix of $A$ in this basis is block-diagonal with $r = [F : K(\alpha)]$ blocks, where each block is a matrix of the left multiplication by $\alpha$ in $K(\alpha)$. So it suffices to prove the lemma for the extension $K(\alpha)/K$. In this case we

choose a basis $1, \alpha, \ldots, \alpha^{k-1}$ of $K(\alpha)$, where $k = [K(\alpha) : K]$. Let $f(x) = x^k + a_1 x^{k-1} + \ldots + a_k$ be the minimal polynomial of $\alpha$. The matrix of $A$ in this basis is

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & -a_k \\ 1 & 0 & \ldots & 0 & -a_{k-1} \\ 0 & 1 & \ldots & 0 & \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_1 \end{bmatrix}$$

So we are done by the previous Lemma. □

§6.3. **Lagrange resolvents.** Let us remind that by Theorem 5.5.1, If $F/K$ is a Galois extension with a cyclic Galois group of order $n$, $K$ contains a primitive $n$-th root of 1, and $\operatorname{char} K$ does not divide $n$ then $F = K(\alpha)$ for some $\alpha \in F$ such that $\alpha^n \in K$. Moreover, the proof is constructive: we show that one can take

$$\alpha = E_\zeta(\beta) = \beta + \zeta^{-1}\sigma(\beta) + \ldots + \zeta^{-(n-2)}\sigma^{n-2}(\beta) + \zeta^{-(n-1)}\sigma^{n-1}(\beta), \quad (12)$$

where $\zeta$ is a primitive $n$-th root of 1 and $\sigma$ is a generator of the Galois group. We proved that $\alpha \neq 0$ for some $\beta$, $\sigma(\alpha) = \zeta\alpha$, $\alpha^n \in K$, and $F = K(\alpha)$. The expression (12) is called a *Lagrange resolvent*.

Let's push this a little bit further. As a function of $\beta$, $E_\zeta(\beta)$ is an $K$-linear function on $F$. We can define $E_{\zeta^k}(\beta)$ for any $0 \leq k < n$ in an obvious way. For example, $E_1(\beta)$ is equal to $\operatorname{Tr}_{F/K}(\beta)$. Introducing a basis of $F$ as a $K$-vector space and the corresponding coordinates, the function

$$E_1(\beta)E_\zeta(\beta)\ldots E_{\zeta^{n-1}}(\beta)$$

is a polynomial (in $n$ coordinates) of degree $n$. Let's assume for simplicity that $K$ is an infinite field. Then this polynomial function does not vanish for some $\beta$. It follows that we can find $\beta \in F$ such that

$$E_1(\beta), E_\zeta(\beta), \ldots, E_{\zeta^{n-1}}(\beta)$$

are non-zero eigenvectors for $\sigma$ with eigenvalues $1, \ldots, \sigma^{n-1}$. It also follows that vectors

$$\beta, \sigma(\beta), \ldots, \sigma^{n-1}(\beta)$$

are linear independent. In fact, their linear independence is equivalent to linear independence of Lagrange resolvents because the transition matrix between the two systems of vectors is the Vandermonde matrix

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & \zeta & \ldots & \zeta^{n-1} \\ 1 & \zeta^2 & \ldots & \zeta^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{n-1} & \ldots & \zeta \end{bmatrix}$$

We have proved a special case of the following quite deep

THEOREM 6.3.1 (Normal Basis Theorem). *Let $F/K$ be a finite Galois extension of degree $n$ with the Galois group $G = \{e = \sigma_0, \sigma_1, \ldots, \sigma_{n-1}\}$. Then there exists $\beta \in F$ such that elements*

$$\beta = \sigma_0(\beta), \sigma_1(\beta), \ldots, \sigma_{n-1}(\beta)$$

*form a basis of $F$ over $K$.*

We will return to this theorem when we discuss representation theory of finite groups.

§6.4. **Solving solvable extensions.** We say that the polynomial equation $f(x) = 0$ is *solvable in radicals* if its splitting field is. By the Galois theorem, this is equivalent to solvability of the Galois group. In problems 11 and 12 from the Homework of §4, you have constructed polynomials over $\mathbb{Q}$ with Galois group $S_n$ for any $n$. If $n > 4$, $S_n$ is not solvable, and therefore this equation is not solvable in radicals. On the other hand, any equation of degree at most 4 is solvable in radicals because its Galois group is a subgroup of $S_4$, and the latter group is solvable.

The proof of the Galois theorem is quite constructive. So one can actually "solve" solvable extensions. Let's consider an equation of degree 3:

$$x^3 + a_1x^2 + a_2x + a_3 = 0 \in K[x].$$

Since we are going to apply the Galois theorem, let's assume right away that $K$ contains a primitive cubic root of unity $\omega$ and that $\operatorname{char} K \neq 2, 3$.

Let $F$ be the splitting field. In this field

$$f(x) = (x - x_1)(x - x_2)(x - x_3).$$

Let $G = \operatorname{Gal}(F/K) \subset S_3$. It is an interesting question to figure out how to compute $G$ in general and it can be solved using the same methods that we use here to compute the roots. So we are just going to assume that

$$G = S_3.$$

Then we have a cyclic tower

$$\{e\} \subset A_3 \subset S_3$$

and the corresponding tower of subfields

$$F \supset F^{A_3} \supset K.$$

The extension $F/F^{A_3}$ has a Galois group $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ which acts by cyclically permuting the roots $x_1 \to x_2 \to x_3 \to x_1$. Let's write down all Lagrange resolvents:

$$\begin{aligned} E_1 &= x_1 + x_2 + x_3 \\ E_\omega &= x_1 + \omega^2 x_2 + \omega x_3 \\ E_{\omega^2} &= x_1 + \omega x_2 + \omega^2 x_3 \end{aligned}$$

It suffices to derive formulas for the Lagrange resolvents, since then we can compute the roots $x_1, x_2, x_3$ by solving a system of linear equations. By Vieta formulas, we have

$$E_1 = -a_1$$

and so it suffices to compute

$$E_\omega^3,\ E_{\omega^2}^3 \in F^{A_3}.$$

The extension $F^{A_3}/K$ is cyclic with a Galois group $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$: this quotient group is generated by a transposition $\sigma$ that exchanges $x_1 \leftrightarrow x_2$.

By our general recipe, instead of computing $E^3_\omega$ and $E^3_{\omega^2}$ we want to compute their Lagrange resolvents

$$E^3_\omega \pm \sigma(E^3_\omega) \quad \text{and} \quad E^3_{\omega^2} \pm \sigma(E^3_{\omega^2}),$$

which have the property that their squares belong to $K$. Here we are a little but lucky because

$$\sigma(E^3_\omega) = \sigma(E_\omega)^3 = (x_2 + \omega^2 x_1 + \omega x_3)^3 = (x_1 + \omega x_2 + \omega^2 x_3)^3 = E^3_{\omega^2}.$$

So the Lagrange resolvents for the second step are simply

$$E^3_\omega \pm E^3_{\omega^2}.$$

It remains to compute these resolvents and then to solve the system of two linear equations in two variables to find $E^3_\omega$ and $E^3_{\omega^2}$. Note that $E^3_\omega + E^3_{\omega^2}$ is invariant under $\sigma$, i.e. it is in fact a symmetric polynomial in $x_1, x_2, x_3$, i.e. it should be possible to express it in terms of coefficients of $f(x)$. We skip this routine calculation. Another resolvent is

$$E^3_\omega - E^3_{\omega^2} = (x_1 + \omega x_2 + \omega^2 x_3)^3 - (x_1 + \omega^2 x_2 + \omega x_3)^3 =$$
$$(\omega - \omega^2)(x_1^2 x_2 - x_1 x_2^2 + x_1 x_3^2 - x_1^2 x_3 + x_2^2 x_3 - x_2 x_3^2) =$$
$$= \sqrt{3}i(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{3}iD,$$

where $D$ is the discriminant. It is a routine calculation to express $D^2$ in terms of coefficients of $f(x)$.

This calculation gives formulas for $x_1, x_2, x_3$ discovered by an amazing Italian mathematician Niccolò Tartaglia and nowdays unfairly attributed to Cardano (who promised Tartaglia to never publish his solution). Tartaglia explained his solution in this beautiful poem.

When the cube and the things together
Are equal to some discrete number,
Find two other numbers differing in this one
Then you will keep this as a habit
That their product should always be equal
Exactly to the cube of a third of the things.
The remainder then as a general rule
Of their cube roots subtracted
Will be equal to your principal thing.
In the second of these acts,
When the cube remains alone
You will observe these other agreements:
You will at once divide the number into two parts
So that the one times the other produces clearly
The cube of a third of the things exactly.
Then of these two parts, as a habitual rule,
You will take the cube roots added together,
And this sum will be your thought.
The third of these calculations of ours
Is solved with the second if you take good care,
As in their nature they are almost matched.
These things I found, and not with sluggish steps,

In the year one thousand five hundred, four and thirty
With foundations strong and sturdy
In the city girdled by the sea.
*Niccolò Tartaglia*

§6.5. **Exercises.**

**1.** Show that $S_n$ is solvable if and only if $n \leq 4$.

**2.** (a) Let $f(x) \in K[x]$ be an irreducible separable polynomial with roots

$$\alpha = \alpha_1, \alpha_2, \dots, \alpha_n \in \bar{K}.$$

Suppose that there exist rational functions $\theta_1(x), \dots, \theta_n(x) \in K(x)$ such that $\alpha_i = \theta_i(\alpha)$ for any $i$. Suppose also that

$$\theta_i(\theta_j(\alpha)) = \theta_j(\theta_i(\alpha))$$

for any $i, j$. Show that $K(\alpha)/K$ is solvable in radicals. Hint: this case was examined by this famous Norwegian mathematician:

(b) Give an example of the situation as in part (a) with $K = \mathbb{Q}$ and such that the Galois group of $f(x)$ is not cyclic. Give a specific polynomial $f(x)$, and compute its roots and functions $\theta_i$.

**3.** Let $F/K$ be a finite Galois extension and let $L$ be an intermediate subfield between $F$ and $K$. Let $H$ be the subgroup of $\mathrm{Gal}(F/K)$ mapping $L$ to itself. Prove that $H$ is the normalizer of $\mathrm{Gal}(F/L)$ in $\mathrm{Gal}(F/K)$.

**4.** Let $F/K$ be a Galois extension with a cyclic Galois group $G$. Let $\sigma$ be a generator of $G$. Show that

$$\mathrm{Ker}[\mathrm{Tr}_{F/K}] = \mathrm{Im}[\mathrm{Id}_F - \sigma].$$

In other words, if $\beta \in F$ then $\mathrm{Tr}_{F/K}(\beta) = 0$ iff $\beta = \alpha - \sigma(\alpha)$ for some $\alpha \in F$.

**5.** Consider the extension $\mathbb{Q} \subset F = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$, where $p$ is a prime and $\zeta_p$ is the primitive $p$-th root of unity. Show that $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic the semidirect product of $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p^*$.

**6.** Let $F/K$ be a Galois extension with a cyclic Galois group $G$ of order $p$, where $\mathrm{char}\, K = p$. Let $\sigma$ be a generator of $G$. (a) Show that there exists $\alpha \in F$ such that $\sigma(\alpha) = \alpha + 1$. (b) Show that $F = K(\alpha)$, where $\alpha$ is a root of $x^p - x - a$ for some $a \in K$.

**7.** Suppose that $\mathrm{char}\, K = p$ and let $a \in K$. Show that the polynomial $x^p - x - a$ either splits in $K$ or is irreducible. Show that in the latter case its Galois group is cyclic of order $p$.

**8.** Let $F/K$ be a Galois extension with a cyclic Galois group $G$. Let $\sigma$ be a generator of $G$. Let $\beta \in F$. (a) There exists $\theta \in F$ such that $\alpha \neq 0$, where

$$\alpha = \theta + \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3(\theta) + \ldots + \beta\sigma(\beta)\ldots\sigma^{n-2}(\beta)\sigma^{n-1}(\theta).$$

(b) Show that $N_{F/K}(\beta) = 1$ if and only if $\beta = \alpha/\sigma(\alpha)$ for some $\alpha \in F$.

**9.** Let $f(x)$ be the minimal polynomial over $\mathbb{Q}$ of $\sqrt[5]{\sqrt[3]{17} + \sqrt[4]{37}}$, where all of the indicated radicals are real. Show that the splitting field of $f(x)$ is solvable over $\mathbb{Q}$.

**10.** Let $K = \mathbb{Q}(\zeta)$, where $\zeta$ is a primitive $n$-th root of unity. Show that if $n = p^r$ for some prime $p$ then $N_{K/\mathbb{Q}}(1 - \zeta) = p$.

**11.** Suppose that $F/K$ and $L/F$ are solvable extensions (recall that this does not mean that these extensions are Galois). Is it true that $L/K$ is a solvable extension?

**12.** Prove that there exist infinitely many pairs of integers $(a, b)$ such that $-4a^3 - 27b^2$ is a square in $\mathbb{Z}$.

**13.** Let $n$ and $m$ be coprime integers. Show that $\Phi_n(x)$ (the $n$-th cyclotomic polynomial) is irreducible over $\mathbb{Q}(\zeta_m)$.

**14.** Let $G$ be a subgroup of the group of automorphisms of $\mathbb{C}(z)$ (rational functions in one variable) generated by automorphisms $z \mapsto 1 - z$ and $z \mapsto 1/z$. Show that $G$ has 6 elements and that the field of invariants $\mathbb{C}(z)^G$ is generated by one function. Find this function.

**15.** Let $f(x) \in K[x]$ be an irreducible polynomial of degree 5 such that its discriminant is a square in $K$. Find all possible Galois groups for its splitting field. For each possible Galois group, give an example of $f(x) \in \mathbb{Q}[x]$ with this Galois group.

## §7. Transcendental Extensions

§7.1. **Transcendental Numbers: Liouville's Theorem.** The field of algebraic numbers $\bar{\mathbb{Q}} \subset \mathbb{C}$ is countable but $\mathbb{C}$ is not. So "most" of complex numbers are transcendental (Cantor, 1874). But it is difficult to prove that this or that number is transcendental, and methods developed to answer these questions have lead to many exciting discoveries in number theory.

The first transcendental number was constructed by Liouville (1844). An irrational number $\alpha \in \mathbb{R}$ is called a *Liouville number* if, for any positive integer $n$, there exist integers $p$ and $q$ with $q > 1$ and such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

In other words, a Liouville number admits an incredibly close approximations by rational numbers. Liouville himself considered a number

$$\alpha = \sum_{j=1}^{\infty} 10^{-j!} = 0.11000100000000000000000001000\ldots,$$

which obviously has this property. Indeed,

$$\sum_{j=1}^{n} 10^{-j!} = \frac{p}{q} \quad \text{where} \quad q = 10^{n!}$$

and

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{10^{(n+1)!-1}} < \frac{1}{q^n}$$

LEMMA 7.1.1. *Liouville numbers are transcendental.*

*Proof.* Suppose that $\alpha$ is algebraic and let $f(x) \in \mathbb{Z}[x]$ be a mutiple of its minimal polynomial. Let $m = \deg f(x)$. Let

$$M := \sup_{|x-\alpha|\leq 1} |f'(x)|.$$

Take $n > 0$ and let $p/q$ be an approximation of $\alpha$ as in the definition of the Liouiville number. We obviously have

$$|f(p/q)| \geq 1/q^m.$$

But by the mean value theorem

$$\frac{1}{q^m} \leq |f(p/q)| = |f(p/q) - f(\alpha)| \leq M\left|\frac{p}{q} - \alpha\right| < \frac{M}{q^n}.$$

If $n$ is large enough, this gives a contradiction. □

It is clear that these Liouville numbers are somewhat artificial. With some effort, one can show that "interesting" numbers, such as $e$ or $\pi$, are not Liouville. For example, one can show that Liouville numbers have unbounded denominators in its continued fraction expansion. For the Euler number $e$, the explicit continued fraction expansion was found by Euler:

$$e = 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1+\dots}}}}}}}}}$$

It has unbounded denominators, but one can still prove using this expansion that $e$ is not a Liouville number.

§7.2. **Hermite's Theorem.** The first proof that $e$ is transcendental was found by Hermite (1873).

*Proof.* For any polynomial $f(x)$, we set

$$F(x) = f(x) + f'(x) + f''(x) + \dots$$

Hermite shows (using iterated integration by parts) the following identity:

$$e^x F(0) - F(x) = e^x \int_0^x e^{-t} f(t)\, dt.$$

Indeed, we have

$$e^x \int_0^x e^{-t} f(t)\, dt = e^x f(0) - f(x) + e^x \int_0^x e^{-t} f'(t)\, dt$$

and then we iterate the process.

Now we assume that $e$ is algebraic, i.e.

$$a_0 + a_1 e + \dots + a_n e^n = 0$$

for some rational numbers $a_i$ with $a_0 \neq 0$. Setting $x = k$ in the identity above, multiplying the equation by $a_k$, and adding these equations gives

$$F(0)\sum_{k=0}^{n} a_k e^k - \sum_{k=0}^{n} a_k F(k) = \sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} f(t)\, dt$$

which gives

$$a_0 F(0) + \sum_{k=1}^{n} a_k F(k) = -\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} f(t)\, dt \tag{13}$$

Now we choose $f(t)$ by setting

$$f(t) = \frac{1}{(p-1)!} t^{p-1} \prod_{k=1}^{n} (k-t)^p,$$

where $p$ is a sufficiently large prime.

CLAIM 7.2.1. *The RHS of* (13) *tends to* $0$ *as the prime* $p$ *increases.*

Indeed,

$$\left| \sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} f(t)\, dt \right| < C \int_0^n |f(t)|\, dt < \frac{C_1 (C_2)^p}{(p-1)!} \to 0.$$

So it suffices to prove the final

CLAIM 7.2.2. *The LHS of* (13) *is a non-zero integer.*

The trick is to show that the LHS is an integer that is not divisible by $p$. Since $f(t)$ has a zero of multiplicity $p-1$ at $t = 0$, we have

$$f^{(k)}(0) = 0, \quad k < p-1,$$

and by the (iterated) differentiation of a product formula

$$f^{(k)}(0) = \binom{k}{p-1} \frac{d^{k-p+1}}{dt^{k-p+1}} \prod_{k=1}^{n} (k-t)^p |_{t=0}, \quad k \geq p-1.$$

So, for example,

$$f^{(p-1)}(0) = (n!)^p.$$

We see that $f^{(k)}(0)$ is integral for any $k$ and that $f^{(p-1)}(0)$ is not divisible by $p$ but $f^{(k)}(0)$ is divisible by $p$ for any $k \neq p-1$ because differentiating the product $\prod_{k=1}^{n}(k-t)^p$ gives a factor of $p$. Therefore $a_0 F(0)$ is integral but not divisible by $p$ (if $p$ is large enough).

Since $f(t)$ has a zero of multiplicity $p$ at $t = m$, $1 \leq m \leq n$, we have

$$f^{(k)}(m) = 0, \quad 0 \leq k \leq p-1$$

and

$$f^{(k)}(m) = -p\binom{k}{p} \frac{d^{k-p}}{dt^{k-p}} \left( t^{p-1} \prod_{\substack{i=1\ldots n \\ i \neq m}} (s-t)^p) \right) \Bigg|_{t=m}, \quad k \geq p,$$

is integral and divisible by $p$. It follows that the LHS of (13) is an integer and is not divisible by $p$. In particular it is not zero. □

In 1982, Lindemann used Hermite's identity above to show that $\pi$ is transcendental as well. In fact, he proved the following:

THEOREM 7.2.3. *If $\alpha_1, \dots, \alpha_r$ are distinct algebraic numbers then $e^{\alpha_1}, \dots, e^{\alpha_r}$ are linearly independent over $\bar{\mathbb{Q}}$.*

The proof is very similar to the proof of Hermite's theorem.

The transcendence of $\pi$ follows by the following trick: the Euler identity

$$e^{\pi i} = -1$$

shows that $e^{\pi i}$ and $e^0$ are linearly dependent over $\bar{\mathbb{Q}}$. It follows that $\pi i$, and therefore $\pi$, is transcendental.

## §7.3. **Transcendence Degree.**

DEFINITION 7.3.1. Let $K/k$ be a field extension and let $S$ be a subset of $K$. We say that $S$ is *algebraically dependent* over $k$ if there exists a non-zero polynomial $f \in k[x_1, \dots, x_n]$ such that

$$f(\alpha_1, \dots, \alpha_n) = 0$$

for some different $\alpha_1, \dots, \alpha_n \in S$. Otherwise, we say that $S$ is *algebraically independent* over $k$.

If $S = \{\alpha\}$ then $S$ is algebraically dependent if and only if $\alpha$ is algebraic over $k$. This can be generalized as follows:

LEMMA 7.3.2. *Let $S = \{\alpha_1, \dots, \alpha_n\} \subset K$. Then $S$ is algebraically independent over $k$ if and only if $\alpha_1$ is not algebraic over $k$, $\alpha_2$ is not algebraic over $k(\alpha_1)$, …, $\alpha_n$ is not algebraic over $k(\alpha_1, \dots, \alpha_{n-1})$. In this case $k(\alpha_1, \dots, \alpha_n)$ is isomorphic to the field $k(x_1, \dots, x_n)$ of rational functions in $n$ variables.*

*Proof.* Suppose that $S$ is algebraically dependent. There exists $\alpha_i$ (perhaps $i = 1$) such that $\alpha_1, \dots, \alpha_{i-1}$ are algebraically independent but $\alpha_1, \dots, \alpha_i$ are algebraically dependent. Let $f(x_1, \dots, x_i) \in k[x_1, \dots, x_i]$ be a non-trivial polynomial such that $f(\alpha_1, \dots, \alpha_i) = 0$. Take

$$g(x_i) := f(\alpha_1, \dots, \alpha_{i-1}, x_i) \in k(\alpha_1, \dots, \alpha_{i-1})[x_i].$$

Since $\alpha_1, \dots, \alpha_{i-1}$ are algebraically independent, $g(x_i) \neq 0$. Since $g(\alpha_i) = 0$, $\alpha_i$ is algebraic over $k(\alpha_1, \dots, \alpha_{i-1})$.

Now suppose that $\alpha_i$ is algebraic over $k(\alpha_1, \dots, \alpha_{i-1})$. Then there exists a non-trivial polynomial $g(x_i) \in k(\alpha_1, \dots, \alpha_{i-1})[x_i]$ such that $g(\alpha_i) = 0$. By clearing denominators, we get a non-trivial polynomial $f \in k[x_1, \dots, x_n]$ such that $f(\alpha_1, \dots, \alpha_n) = 0$.

Consider the homomorphism $k[x_1, \dots, x_n] \to K$ that sends $x_i$ to $\alpha_i$. Its kernel is trivial by definition of algebraic independence. Therefore, we have an induced embedding of the field of fractions $k(x_1, \dots, x_n) \hookrightarrow K$. The image is equal to $k(\alpha_1, \dots, \alpha_n)$. □

DEFINITION 7.3.3. An algebraically independent subset $S \subset K$ is called a *transcendence basis* if $K$ is algebraic over $k(S)$. The cardinality of any transcendence basis is called the *transcendence degree* of $K/k$ (we will prove that it does not depend on $S$). Notation: $\mathrm{tr.deg.}(K/k)$

The concept of algebraic dependence is similar to the concept of linear dependence but in a slightly non-trivial way. Here are some parallels:

| Linear algebra | Fields |
|---|---|
| vector space $V$ | Field extension $K/k$ |
| linearly independent subsets | algebraically independent subsets |
| $v \in \mathrm{Span}\{u_1, \ldots, u_n\}$ | $\beta$ is algebraic over $k(\alpha_1, \ldots, \alpha_n)$ |
| basis | transcendence basis |
| dimension | transcendence degree |

There is a good reason for this analogy: just like the number of elements in any basis of a vector space computes its dimension, the transcendence degree of a field extension computes the dimension of the algebraic set. We will discuss this correspondence in the next chapter.

Now the main result:

THEOREM 7.3.4. *Suppose there exists a finite subset $S \subset K$ such that $K$ is algebraic over $k(S)$. Then $K$ admits a finite transcendence basis, and all these bases have the same number of elements (i.e. the transcendence degree is well-defined).*

*Proof.* We can assume that $S$ is the minimal (by inclusion) subset such that $K$ is algebraic over $k(S)$. If $S = \{\alpha_1, \ldots, \alpha_n\}$ is algebraically independent then $S$ is a transcendence basis, by definition. Suppose it is algebraically dependent. After renumbering, we can assume that $\alpha_n$ is algebraic over $k(\alpha_1, \ldots, \alpha_{n-1})$. Then $K$ is algebraic over $k(\alpha_1, \ldots, \alpha_{n-1})$. It follows that $S$ is not the minimal subset such that $K$ is algebraic over $k(S)$, a contradiction.

The fact that all transcendence bases have the same number of elements is a bit subtle (just like the fact that dimension of a vector space is well-defined is a bit subtle) and follows from Lemma 7.3.6, which in turn follows from the basic Exchange Lemma below. □

LEMMA 7.3.5 (Exchange property). *Let $\{\alpha_1, \ldots, \alpha_m\}$ be a subset of $K$. If $\beta \in K$ is algebraic over $k(\alpha_1, \ldots, \alpha_m)$ but not over $k(\alpha_1, \ldots, \alpha_{m-1})$ then $\alpha_m$ is algebraic over $k(\alpha_1, \ldots, \alpha_{m-1}, \beta)$.*

*Proof.* By shrinking, we can assume that $\alpha_1, \ldots, \alpha_{m-1}$ are algebraically independent. It follows that $\alpha_1, \ldots, \alpha_{m-1}, \beta$ are algebraically independent. Let $f \in k[x_1, \ldots, x_m, y]$ be a polynomial such that

$$f(\alpha_1, \ldots, \alpha_m, y) \neq 0, \quad f(\alpha_1, \ldots, \alpha_m, \beta) = 0.$$

Then

$$f = \sum g_i(x_1, \ldots, x_{m-1}, y) x_m^i.$$

Take $i$ such that $g_i \neq 0$. Since $\alpha_1, \ldots, \alpha_{m-1}, \beta$ are algebraically independent, we have

$$g_i(\alpha_1, \ldots, \alpha_{m-1}, \beta) \neq 0.$$

Therefore, $f(\alpha_1, \ldots, \alpha_{m-1}, x_m, \beta)$ is a non-trivial polynomial which vanishes for $x_m = \alpha_m$. So $\alpha_m$ is algebraic over $k(\alpha_1, \ldots, \alpha_{m-1}, \beta)$. □

LEMMA 7.3.6. *If $A = \{\alpha_1, \ldots, \alpha_m\}$ and $B = \{\beta_1, \ldots, \beta_n\}$ are subsets of $K$ such that*

- *$A$ is algebraically independent and*
- *every element of $A$ is algebraic over $k(B)$,*

*then $m \leq n$.*

*Proof.* If $A \subset B$ then there is nothing to prove. We will reduce to this case by applying the exchange property several times. After renumbering, suppose that

$$B = \{\alpha_1, \dots, \alpha_k, \beta_{k+1}, \dots, \beta_n\},$$

where $\beta_i \notin A$ for $i \geq k+1$. Since $\alpha_{k+1}$ is algebraic over $k(B)$ but not over $k(\alpha_1, \dots, \alpha_k)$, there exists some $\beta_i$ for $i \geq k+1$ such that $\alpha_{k+1}$ is algebraic over $k(\alpha_1, \dots, \alpha_k, \beta_{k+1}, \dots, \beta_i)$ but not over $k(\alpha_1, \dots, \alpha_k, \beta_{k+1}, \dots, \beta_{i-1})$. By exchange lemma, $\beta_i$ is algebraic over

$$B_1 = B \cup \{\alpha_{k+1}\} \setminus \{\beta_i\}.$$

Therefore any element of $B$ is algebraic over $k(B_1)$. By transitivity of algebraic dependence, any element of $A$ is algebraic over $k(B_1)$. Notice that $B_1$ and $B$ have the same number of elements but $A$ and $B_1$ have more elements in common than $A$ and $B$. □

## §8. Algebraic Sets

### §8.1. **Noether's Normalization Lemma.** Theorem 7.3.4 has a basic

COROLLARY 8.1.1. *Let $K$ be a finitely generated field extension of $k$. Then $K$ contains algebraically independent over $k$ elements $x_1, \dots, x_n$ such that $K$ is a finite algebraic extension of $k(x_1, \dots, x_n)$*

For $k$-algebras, we have the following more precise result.

LEMMA 8.1.2 (Noether's Normalization Lemma). *Let $A$ be a finitely generated $k$-algebra. Then $A$ contains algebraically independent over $k$ elements $x_1, \dots, x_n$ such that $A$ is integral over $k[x_1, \dots, x_n]$*

Recall that a $k$-algebra $A$ is a ring that contains $k$. It is finitely generated if it contains elements $y_1, \dots, y_r$ such that any element of $A$ is a polynomial in $y_1, \dots, y_r$ with coefficients in $k$. This can be expressed by saying that $A = k[y_1, \dots, y_r]$ but this notation is a bit ambiguous: $A$ is isomorphic to the algebra of polynomials in $r$ variables only if $y_1, \dots, y_r$ are algebraically independent. In general, $A$ is only a quotient algebra of the algebra of polynomials in $r$ variables by some ideal $I$. These algebras are very important in geometry, because they serve as algebras of functions of algebraic sets given by vanishing of polynomials in $I$ (under some mild conditions on $I$ to be discussed later).

Recall that an element $a \in A$ is *integral* over a subring $B \subset A$ if $a$ is a root of a *monic* polynomial with coefficients in $B$. The only difficulty in the proof of Noether's normalization lemma is to convert an algebraic relation

$$f(y_1, \dots, y_r) = 0$$

between generators into an integral dependence relation of one of the generators, something like

$$y_r^N + g_1(y_1, \dots, y_{r-1}) y_r^{N-1} + \dots + g_N(y_1, \dots, y_{r-1}) = 0.$$

It turns out that this is possible after a very simple "change of variables".

*Proof.* Suppose that $k$ is an infinite field (see exercises for a finite field case). Let $y_1, \dots, y_r$ be generators of $A$ over $k$. We argue by induction on $r$. If $r = 1$ there is nothing to prove. If $y_1, \dots, y_r$ are algebraically independent then again there is nothing to prove. Suppose we have a polynomial equation

$$f(y_1, \dots, y_r) = 0.$$

Let $F(y_1, \dots, y_r)$ be the homogeneous component of $f$ of top degree. Then $F(y_1, \dots, y_{r-1}, 1)$ is a non-trivial polynomial. Since $k$ is infinite, we can find $\lambda_1, \dots, \lambda_{r-1} \in k$ such that

$$F(\lambda_1, \dots, \lambda_{r-1}, 1) \neq 0.$$

Now we introduce new elements $y'_1, \dots, y'_{r-1} \in A$ by formulas

$$y_1 = y'_1 + \lambda_1 y_r, \dots, y_{r-1} = y'_{r-1} + \lambda_{r-1} y_r.$$

We notice that $y'_1, \dots, y'_{r-1}, y_r$ generate $A$ and we have

$$g(y'_1, \dots, y'_{r-1}, y_r) := f(y'_1 + \lambda_1 y_r, \dots, y'_{r-1} + \lambda_{r-1} y_r, y_r) = 0.$$

As a polynomial in $y_r$, $g$ has top coefficient $F(\lambda_1, \dots, \lambda_{r-1}, 1) \neq 0$. So $A$ is integral over a subalgebra $A'$ generated by $y'_1, \dots, y'_{r-1}$. By induction, $A'$ is integral over its subalgebra $B$ generated by algebraically independent elements $x_1, \dots, x_n$. By transitivity of integral dependence, $A$ is integral over $B$ as well. □

§8.2. **Weak Nullstellensatz.** One of the main ideas of algebraic geometry is to build a vocabulary that relates geometric properties of "spaces $X$" and algebraic properties of their "rings of functions $\mathcal{O}(X)$". As a basic example, lets fix a field $k$ and consider an affine space over this field:

$$\mathbb{A}^n.$$

Of course points of $\mathbb{A}^n$ are just $n$-tuples $(a_1, \dots, a_n) \in k^n$, but we don't care much about the vector space structure here, so the notation $\mathbb{A}^n$ is more convenient. We consider only polynomial functions in algebraic geometry, so we take

$$\mathcal{O}(\mathbb{A}^n) = k[x_1, \dots, x_n].$$

THEOREM 8.2.1 (Weak Nullstellensatz). *If $k$ is algebraically closed then there is a 1-1 correspondence between points of $\mathbb{A}^n$ and maximal ideals of $\mathcal{O}(\mathbb{A}^n)$. More precisely, a point of $\mathbb{A}^n$ corresponds to the maximal ideal that consists of all polynomials that vanish at this point.*

*Proof.* Given a point $a = (a_1, \dots, a_n)$, consider an evaluation homomorphism

$$\psi : k[x_1, \dots, x_n] \to k, \quad x_i \mapsto a_i.$$

It is surjective onto a field, and so its kernel is a maximal ideal.

Now suppose that $\mathfrak{m} \subset k[x_1, \dots, x_n]$ is a maximal ideal such that

$$k[x_1, \dots, x_n]/\mathfrak{m} \simeq k.$$

Consider the corresponding homomorhism $\psi : k[x_1, \dots, x_n] \to k$ and let $a_i := \psi(x_i)$. Then $\psi$ is completely determined by $a_1, \dots, a_n$, and therefore $\psi$ is an evaluation map at the point $(a_1, \dots, a_n)$ of $\mathbb{A}^n$.

Next we notice that if $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ is *any* maximal ideal then $A := k[x_1, \ldots, x_n]/\mathfrak{m}$ is a field that contains $k$, and which is finitely generated over $k$. Since $k$ is also algebraically closed, everything follows from the following lemma. □

LEMMA 8.2.2. *If $A$ is a finitely generated $k$ algebra and a field, then $A$ is a finite algebraic extension of $k$. In particular, if $k$ is algebraically closed them $A = k$.*

*Proof.* By Noether's normalization lemma, $A$ is integral over its subalgebra $B = k[x_1, \ldots, x_r]$, where $x_1, \ldots, x_r$ are algebraically independent over $k$. Let $\alpha \in B$. Since $A$ is a field, $1/\alpha$ is in $A$. Since $A$ in integral over $B$, $1/\alpha$ satisfies a monic equation

$$(1/\alpha)^n + b_1(1/\alpha)^{n-1} + \ldots + b_n, \quad b_i \in B.$$

Multiplying by $\alpha^{n-1}$, this gives

$$1/\alpha = -b_1 - \ldots - b_n\alpha^{n-1} \in B,$$

i.e. $B$ is a field as well. But this is impossible unless $r = 0$, because $B$ is isomorphic to the algebra of polynomials in $r$ variables. So $A$ is integral over $k$. It follows that $A$ is a finite algebraic extension of $k$. □

§8.3. **Affine Algebraic Sets. Strong Nullstellensatz.** The fundamental theorem of algebra can be rephrased by saying that there is a bijection between polynomials $f \in \mathbb{C}[x]$ (up to a scalar multiple) and its roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ (with multiplicities). In other words, there is a bijection between proper ideals $A \in k[x]$ (algebra) and finite subsets of points in $k$ with multiplicities (geometry). Let's see how to generalize this to higher dimensions.

Let $k$ be an algebraically closed field.

DEFINITION 8.3.1. A subset $X \subset k^n$ is called *closed algebraic* if there exist polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ such that

$$X = \{(a_1, \ldots, a_n) \,|\, f_i(a_1, \ldots, a_n) = 0 \text{ for any } i\}.$$

This subset depends only on the ideal $A = (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$ and not on the actual polynomials. So alternatively, we can also define closed algebraic subsets as subsets of the form

$$V(A) = \{(a_1, \ldots, a_n) \,|\, f(a_1, \ldots, a_n) = 0 \text{ for any } f \in A\},$$

where $A$ is a fixed ideal. By the Hilbert basis theorem, any ideal $A$ is finitely generated by some $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, so this definition is the same as above.

If $X$ is a closed algebraic subset, we can take a look at all polynomial functions that vanish at $X$:

$$I(X) = \{f \in k[x_1, \ldots, x_n] \,|\, f(a_1, \ldots, a_n) = 0 \text{ for any } (a_1, \ldots, a_n) \in X\}.$$

It is clear that $A \subset I(V(A))$. The precise relationship is given by

THEOREM 8.3.2 (Strong Nullstellensatz).

$$I(V(A)) = \sqrt{A} := \{g \in k[x_1, \ldots, x_n] \,|\, g^l \in A \text{ for some integer } l\}.$$

*Proof.* It is clear that $\sqrt{A} \subset I(V(A))$. So we only have to show the other inclusion. The Nullstellensatz has many proofs, but we we will follow one particularly nice approach known as "Rabinowitch's trick". In concrete terms, we have to show the following. Let $A = (f_1, \dots, f_m)$ and suppose that $g \in k[x_1, \dots, x_n]$ vanishes at any point $(a_1, \dots, a_n)$ where each $f_i$ vanishes. Then we claim that there exists an integer $l$ and polynomials $h_1, \dots, h_m$ such that

$$g^l = \sum h_i f_i.$$

We introduce the ideal

$$B = (f_1, \dots, f_m, 1 - gx_{n+1}) \subset k[x_1, \dots, x_{n+1}].$$

We claim that $B = k[x_1, \dots, x_{n+1}]$. If not then $B$ is contained in a maximal ideal $\mathfrak{m}$. By the weak Nullstellensatz, $\mathfrak{m}$ consists of all polynomials that vanish at some point $(a_1, \dots, a_{n+1})$. But then $f_i(a_1, \dots, a_n) = 0$ for any $i$ but $g(a_1, \dots, a_n)a_{n+1} = 1$. This is a contradiction because $g(a_1, \dots, a_n) = 0$.

It follows that we can find polynomials $h_1, \dots, h_{m+1} \in k[x_1, \dots, x_{n+1}]$ such that

$$\sum h_i f_i + h_{m+1}(1 - gx_{n+1}) = 1.$$

The trick is to substitute $1/g$ for $x_{n+1}$ in this formula. This gives

$$\sum h_i(x_1, \dots, x_n, 1/g) f_i(x_1, \dots, x_n) = 1.$$

Clearing denominators (i.e. multiplying by a sufficiently large power of $g$), this gives

$$\sum h_i^*(x_1, \dots, x_n) f_i(x_1, \dots, x_n) = g^l(x_1, \dots, x_n)$$

for some new polynomials $h_1^*, \dots, h_m^*$. □

COROLLARY 8.3.3. *Operations V and I set up a bijection between closed algebraic subsets of $\mathbb{A}^n$ and ideals $A \subset k[x_1, \dots, x_n]$ such that $A = \sqrt{A}$.*

Ideals $A$ such that $A = \sqrt{A}$ are sometimes called *radical ideals*.

*Proof.* Let $A = \sqrt{A}$. By the strong Nullstellensatz, we have

$$I(V(A)) = \sqrt{A} = A.$$

Now suppose that $X = V(B)$ is an algebraic set. Then, clearly, $I(X)$ is radical and by the strong Nullstellensatz,

$$V(I(X)) = V(\sqrt{B}) = V(B) = X.$$

□

§8.4. **Preview of Schemes: a double point.** $\operatorname{MaxSpec} \mathbb{Z}$**.** The Nullstellensatz shows that there is a bijection between algebraic subsets $X \subset \mathbb{A}^n$ and radical ideals in $k[x_1, \dots, x_n]$ that sends $X$ to $I(X)$. Geometric properties of $X$ are encoded in algebraic properties of its algebra of polynomial functions

$$\mathcal{O}(X) = k[x_1, \dots, x_n]/I(X).$$

In the one-dimensional case, algebraic subsets $A \subset \mathbb{A}^1$ are just finite collections of points $\alpha_1, \dots, \alpha_n \in \mathbb{A}^1$. Then $I(X)$ is the ideal generated by a square-free polynomial $(x - \alpha_1) \dots (x - \alpha_n)$. To ignore multiplicities, we

had to shrink the set of interesting ideals. Another approach is to keep all ideals and to enhance geometry by considering points with multiplicities. A systematic development of this idea leads to the theory of algebraic schemes. To get its flavor, let us consider a double point, i.e. a point in $\mathbb{A}^1$ (for instance the origin) of multiplicity 2.

The corresponding ideal is $(x^2) \subset k[x]$. For a simple point, the algebra of functions $k[x]/(x) \simeq k$ consists of constants only. But for the double point we get the *algebra of dual numbers*

$$k[x]/(x^2) = \{a + b\varepsilon \,|\, \varepsilon^2 = 0\}.$$

For a simple point, the restriction homomorphism $k[x] \to k$ just sends a function $f$ to its value (at 0):

$$k[x] \to k, \quad f(x) \mapsto f(0)$$

But for a double point, the restriction homomorphism, by the Tailor formula, is

$$f(x) \mapsto f(0) + f'(0)\varepsilon$$

This is often phrased by saying that a double point is a point plus a tangent vector to $\mathbb{A}^1$ at this point. A double point knows not just how to evaluate a function, but also how to take a derivative of a function in a given direction! In other words, a double point can be thought of as a very small "$\varepsilon$-neighborhood" of a point, which is big enough to compute a derivative of any function, but too small to compute derivatives of higher order.

If one starts with any ring $R$, the Nullstellensatz paves a way to construct a geometric object that encodes algebraic properties of $R$. In fact, there is an hierarchy of geometric objects that encode algebra of $R$ better and better. The first approximation is to take a maximal spectrum of $R$:

$$\mathrm{MaxSpec}(R) = \{\mathfrak{m} \subset R \,|\, \mathfrak{m} \text{ is a maximal ideal}\}.$$

For example, if $X \subset \mathbb{A}^n$ is an algebraic set and $R = k[x_1, \dots, x_n]/I(X)$ then the maximal ideals of $R$ correspond to maximal ideals of $k[x_1, \dots, x_n]$ that contain $I(X)$. By the weak Nullstellensatz, this gives a bijection

$$\mathrm{MaxSpec}(R) = \{(a_1, \dots, a_n) \in \mathbb{A}^n \,|\, f(a_1, \dots, a_n) = 0 \text{ for any } f \in I(X)\}.$$

By Corollary 8.3.3, it follows that

$$\mathrm{MaxSpec}(R) = X.$$

What if we take $R = \mathbb{Z}$? Then

$$\mathrm{MaxSpec}(R) = \{(p) \; p \text{ is a prime number}\}.$$

Any number $n \in \mathbb{Z}$ can be thought of as a function on $\mathrm{MaxSpec}(R)$:

$$(p) \in \mathrm{MaxSpec}(R) \qquad \mapsto \qquad n + (p) \in \mathbb{Z}/p\mathbb{Z}.$$

Notice that this function is a bit unusual from the calculus perspective: it takes values in different fields at different points!

What are the "zeros" of $n \in \mathbb{Z}$? Those are points where the function vanishes, i.e. $(p)$ such that $p|n$. The fundamental theorem of arithmetic can be interpreted by saying that any $n \in \mathbb{Z}$ is uniquely determined by its "roots", i.e. by primes appearing in its prime decomposition. We can also attach multiplicities to prime numbers in the obvious way. So we see

that the fundamental theorems of arithmetic and of algebra geometrically encode very similar statements in the spirit of Nullstellensatz.

§8.5. **Exercises.**

**1.** Let $S$ be a finite set and let $\mathcal{I}$ be a non-empty collection of its subsets (called the independent sets). A pair $(S, \mathcal{I})$ is called a *finite matroid* if

- every subset of an independent set is independent;
- Exchange property: If $A$ and $B$ are independent sets and $|A| > |B|$ then there exists $x \in A \setminus B$ such that $B \cup \{x\}$ is independent.

Show that the following pairs are matroids. (a) $S$ is the set of columns of a matrix $A$ over a field $k$; $\mathcal{I}$ is the collection of linearly independent subsets of columns. (b) Let $K/k$ be a field extension and let $S \subset K$ be a finite subset. Let $\mathcal{I}$ be the collection of algebraically independent subsets of $S$. (c) Let $S$ be a set with $n$ elements and let $\mathcal{I}$ be the collection of subsets with at most $r$ elements (a uniform matroid). (d) Let $S$ be the set of edges of a finite graph. Let $\mathcal{I}$ be the collection of subsets of edges that do not contain cycles.

**2.** Let $(S, \mathcal{I})$ be a finite matroid. A maximal (by inclusion) independent subset is called a basis of the matroid. Show that any two bases have the same number of elements (called the rank of the matroid).

**3.** (a) Define the notion of isomorphic matroids. (b) Let $(S, \mathcal{I})$ be a uniform matroid of rank 2 (as in 1c). Show that $S$ is isomorphic to a matroid of type 1a with $k = \mathbb{F}_q$ if and only if $|S| \leq q + 1$. (c) Show that any matroid of type 1d is isomorphic to a matroid of type 1a with $k = \mathbb{F}_2$ (Hint: the matrix $A$ has a simple meaning in terms of the graph).

**4.** Let $\mathcal{B}$ be a non-empty collection of subsets of a finite set $S$. Show that $\mathcal{B}$ is a collection of bases of some matroid if and only if for any $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, there exists $y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

**5.** Let $x$ be transcendental over $k$ and let $F \subset k(x)$ be a subfield properly contaning $k$. Show that $k(x)$ is finite-dimensional over $F$.

**6.** Let $K_1$ and $K_2$ be algebraically closed extensions of $\mathbb{C}$ of transcendence degree 11. Let $f : K_1 \to K_2$ be a homomorphism. Show that $f$ is an isomorphism.

**7.** Let $k \subset K \subset E$ be field extensions with $\mathrm{tr.deg.}\, E/k < \infty$. Show that

$$\mathrm{tr.deg.}\, E/k = \mathrm{tr.deg.}\, K/k + \mathrm{tr.deg.}\, E/K.$$

**8.** Prove the Noether normalization theorem when $k$ is a finite field. Hint: instead of the substitution $y_i' = y_i - \lambda_i y_k$ (with $\lambda_i \in k$), use the substitution $y_i' = y_i - y_k^{n_i}$ for appropriate powers $n_i$.

**9.** (a) Let $A \subset B$ be domains and suppose that $B$ is integral over $A$. Show that $A$ is a field if and only if $B$ is a field. (b) Let $A \subset B$ be rings and suppose that $B$ is integral over $A$. Let $\mathfrak{p} \subset B$ be a prime ideal. Show that $\mathfrak{p}$ is a maximal ideal of $B$ if and only if $\mathfrak{p} \cap A$ is a maximal ideal of $A$.

**10.** (a) Let $A$ be an integrally closed domain with the field of fractions $K$. Let $F/K$ be a Galois extension with the Galois group $G$. Let $B$ be the integral closure of $A$ in $F$. Show that $G$ preserves $B$ and that $B^G = A$. (b) Deduce from part (a) that the ring of invariants $k[x_1, \ldots, x_n]^{S_n}$ is generated by elementary symmetric functions $\sigma_1, \ldots, \sigma_n$.

**11.** Let $A$ be a finitely generated $k$-algebra and let $B \subset A$ be a subalgebra such that $A$ is integral over $B$. Show that $A$ is a finitely generated $B$-module and $B$ is a finitely generated $k$-algebra (Hint: consider a subalgebra of $B$ generated by coefficients of monic equations satisfied by generators of $A$).

**12.** Let $f, g \in \mathbb{C}[x, y]$ and suppose that $f$ is irreducible and does not divide $g$ in $\mathbb{C}[x, y]$. (a) Show that $f$ is still irreducible and does not divide $g$ in $\mathbb{C}(x)[y]$. (b) Show that

$$V(f, g) = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = g(x, y) = 0\}$$

is a union of finitely many points.

**13.** Let $\mathfrak{p} \subset \mathbb{C}[x, y]$ be a prime ideal. Show that either $\mathfrak{p} = \{0\}$ or $\mathfrak{p}$ consists of all polynomials vanishing at some point $(a, b) \in \mathbb{C}^2$ or $\mathfrak{p} = (f)$, where $f \in \mathbb{C}[x, y]$ is an irreducible polynomial.

## §9. Geometry and Commutative Algebra

### §9.1. **Localization and Geometric Intuition Behind It.**

Example 9.1.1 (Number Theory). The most familiar example of localization is a formation of rational numbers as fractions of integers: $\mathbb{Z} \subset \mathbb{Q}$. There are many intermediate subrings between $\mathbb{Z}$ and $\mathbb{Q}$ that can be formed by restricting what kind of denominators we want. For example, we can invert only 2:

$$\mathbb{Z}[1/2] = \left\{ \frac{a}{2^n} \mid a \in \mathbb{Z}, \quad n \geq 0 \right\} \subset \mathbb{Q}.$$

Or we can invert everything *coprime* to 2 (i.e. odd):

$$\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, \quad b \notin (2) \right\} \subset \mathbb{Q}.$$

This ring has only one maximal ideal, namely a principal ideal generated by 2. Indeed, any element not in this ideal is a unit, and so can not be contaned in a proper ideal. $\mathbb{Z}_{(2)}$ is an example of a *local ring*:

Definition 9.1.2. A ring $R$ is called local if it has only one maximal ideal.

Example 9.1.3 (Geometry). What is the geometry behind this? In geometry we often study spaces *locally*, i.e. in neighborhoods of points. What are these neighborhoods in algebraic geometry? Consider the affine line $\mathbb{A}^1$ with ring of functions $k[x]$. We want to define neighborhoods of 0. We had a definition of a closed algebraic set, in this case just a finite set of points. Complements of closed algebraic sets are called *Zariski open sets*. They form a topology, called *Zariski topology*. So neighborhoods of 0 look like $\mathbb{A}^1 \setminus \{\alpha_1, \ldots, \alpha_r\}$, for example $U = \mathbb{A}^1 \setminus \{1\}$. What are the functions on this neighborhood? We are algebraists, so interested in polynomial or rational functions, and here we can take

$$\mathcal{O}_U = k\left[x, \frac{1}{x-1}\right],$$

i.e. rational functions with poles only at 1. More generally, for $U = \mathbb{A}^1 \setminus \{\alpha_1, \ldots, \alpha_r\}$ we will get

$$\mathcal{O}_U = k\left[x, \frac{1}{x-\alpha_1}, \ldots, \frac{1}{x-\alpha_r}\right].$$

Let's go even further and invert all polynomials that don't vanish at $0$:

$$k[x]_{(x)} = \left\{ \frac{f(x)}{g(x)} \mid g(x) \neq 0 \right\}.$$

So we take all functions defined in some Zariski neighborhood of $0$ (that depend on a function: have to throw away all roots of the denominator). This is again a local ring: the only one maximal ideal consists of fractions such that $f(0) = 0$, i.e. such that $f(x) \in (x) \subset k[x]$.

A useful intuition is to think about $k[x]_{(x)}$ as functions on a small "local" neighborhood of $0 \in \mathbb{A}^1$, even though there is no Zariski neighborhood that we can use for this purpose.

Now let's give a general algebraic definition.

DEFINITION 9.1.4. A subset $S \subset R$ is called a multiplicative system if

- If $s, t \in S$ then $st \in S$.
- $1 \in S$, $0 \notin S$.

A multiplicative system is the set of future "denominators", i.e. things that we want to invert. We define a localization $S^{-1}R$ as a set of equivalence classes of fractions $r/s$, where $r \in R$, $s \in S$, such that two fractions $r/s$ and $r'/s'$ are considered equivalent if there exists $t \in S$ such that

$$t(s'r - sr') = 0.$$

Notice that if $R$ is a domain then of course we can take $t = 1$, but in general we have to modify the usual cross-multiplication formula as above. We define ring operations on $R$ as usual addition and multiplication of fractions. One has to check that these operations are well-defined. Finally, we have a homomorphism

$$R \to S^{-1}R, \quad r \mapsto r/1.$$

If $R$ is not a domain, this homomorphism is not necessarily injective.

LEMMA 9.1.5. *The ring $S^{-1}R$ is well-defined.*

*Proof.* This is a bit tedious, but done in class. □

EXAMPLE 9.1.6. Let $R$ be a domain, $S = R \setminus \{0\}$. Then $S^{-1}R$ is the quotient field of $R$. More generally, if $R$ is not necessarily a domain, one can take $S$ to be the set of non-zerodivisors (this is the largest set we can hope to invert). Then $S^{-1}R$ is called a *total ring of fractions*.

EXAMPLE 9.1.7. Suppose $x \in R$ is not a nilpotent. Then

$$S = \{1, x, x^2, x^3, \ldots\}$$

is a multiplicative system. The corresponding localization $S^{-1}R$ is often denoted by $R[1/x]$.

Finally, here is perhaps the most important example:

EXAMPLE 9.1.8. Let $\mathfrak{p} \subset R$ be a prime divisor, i.e.

$$\text{if } xy \in \mathfrak{p} \text{ then either } x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}.$$

Taking a contrapositive of this statement shows that

$$S = R \setminus \mathfrak{p}$$

is a multiplicative system. There is a special notation for $S^{-1}R$: it is denoted by $R_{\mathfrak{p}}$ and called *localization of $R$ at $\mathfrak{p}$*.

EXAMPLE 9.1.9. For a concrete example of $R_{\mathfrak{p}}$, take $(x) \subset k[x]$, i.e. the ideal of polynomial functions that vanish at $0 \in \mathbb{A}^1$. Then $k[x]_{(x)}$ is the ring of all fractions $f(x)/g(x)$ such that $g(x) \notin (x)$, i.e. such that $g(0) \neq 0$. Intuitively, ring $k[x]_{(x)}$ is the ring of functions on a very small "local" neighborhood of $0 \in \mathbb{A}^1$ (although there is no Zariski neighborhood with this property).

Let us give a very concrete characterization of the localization:

LEMMA 9.1.10. *Let $f : R \to S^{-1}R$ be the localization. Then*

- *$f(s)$ is a unit for any $s \in S$.*
- *$f(a) = 0$ if and only if $sa = 0$ for some $s \in S$.*
- *any element of $S^{-1}R$ can be written as $f(a)/f(s)$ for some $a \in R$, $s \in S$.*

*Conversely, if a homomorphism $f : R \to A$ has these properties then $A \simeq S^{-1}R$.*

*Proof.* We have $(s/1)(1/s) = 1$ in $S^{-1}R$. So $f(s)$ is a unit. The fractions $a/1$ and $0/1$ give the same element of $S^{-1}R$ if and only if $sa = 0$ for some $s \in S$, by definition of $S^{-1}R$.

Now suppose that a homomorphism $f : R \to A$ has these properties. We construct a map $g : S^{-1}R \to A$ by formula $g(r/s) = f(r)f(s)^{-1}$. This is well-defined: if $r/s = r'/s'$ then $t(s'r - sr') = 0$ for some $t \in S$. Applying a homomorphism $f$ gives

$$f(t)(f(s')f(r) - f(s)f(r')) = 0$$

in $A$, which implies that $f(r)f(s)^{-1} = f(r')f(s')^{-1}$ because $f(s)$, $f(s')$, and $f(t)$ are invertible. □

§9.2. **Ideals in $R$ and in $S^{-1}R$.** .

It is useful to understand the relationship between ideals of $R$ and $S^{-1}R$.

DEFINITION 9.2.1. For any ideal $I \subset R$, let $S^{-1}I \subset S^{-1}R$ be the subset of fractions of the form $\frac{x}{s}$ with $x \in I$. One checks immediately that $S^{-1}I$ is an ideal. Namely, if $\frac{x}{s}, \frac{x'}{s'} \in S^{-1}I$ then $s'x + sx' \in I$ and therefore

$$\frac{x}{s} + \frac{x'}{s'} = \frac{s'x + sx'}{ss'} \in S^{-1}I.$$

And if $\frac{r}{t} \in S^{-1}R$ then $\frac{r}{t}\frac{x}{s} = \frac{rx}{ts} \in S^{-1}I$ because $rx \in I$. The ideal $S^{-1}I$ is called *an extended ideal*.

There is also a map in the opposite direction. Let $f : R \to S^{-1}R$ be a canonical map. If $J \subset S^{-1}R$ is an ideal then the ideal $f^{-1}(J) \subset R$ is called a *contracted ideal*. Abusing notation, it is often denoted by $J \cap R$.

REMARK 9.2.2. One can define contraction and extension in a much more general setting: if $f : A \to B$ is any homomorphism of rings, the we have a contraction map $J \mapsto f^{-1}(J)$ from the set of ideals of $B$ to the set of ideals of $A$ and the extension map $I \mapsto Bf(I)$ from the set of ideals of $A$ to the set of ideals of $B$, where $Bf(I)$ is the minimal ideal in $B$ containing $f(I)$ (which is almost never an ideal itself unless $f$ is surjective).

PROPOSITION 9.2.3. *We have the following properties:*

- *The mapping $I \mapsto S^{-1}I$ is $1:1$ mapping of the set of all contracted ideals of $R$ (i.e. ideals of the form $R \cap J$) to the set of all ideals of $S^{-1}R$.*
- *Prime ideals of $S^{-1}R$ are in $1:1$ correspondence ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) with prime ideals of $R$ that don't intersect $S$.*

*Proof.* Let $J \subset S^{-1}R$ be an ideal and let $r/s \in J$. Then $r = s(r/s) \in J$, and therefore $r \in R \cap J$. It follows that $J \subset S^{-1}(R \cap J)$. The other inclusion is obvious, and so we have

$$J = S^{-1}(R \cap J).$$

This proves the first part.

For the second part, if $I \subset R$ is any ideal that intersects $S$ then $S^{-1}I = R^{-1}S$ is not proper. We claim that if $\mathfrak{p} \subset R$ is a prime ideal that does not intersect $S$ then $S^{-1}\mathfrak{p}$ is also prime. Indeed, suppose we have

$$\frac{r}{s}\frac{r'}{s'} = \frac{x}{t},$$

where $x \in \mathfrak{p}$. Then $u(trr' - xss') = 0$ for some $u \in S$. It follows that $trr' - xss' \in \mathfrak{p}$, and therefore $trr' \in \mathfrak{p}$. This implies that $r$ or $r'$ is in $\mathfrak{p}$, i.e. $\frac{r}{s}$ or $\frac{r'}{s'}$ is in $S^{-1}\mathfrak{p}$. In the other direction, if $J \subset S^{-1}R$ is a prime ideal then $R \cap J$ is also a prime ideal. This is true for any homomorphism $f : A \to B$: if $J \subset B$ is a prime ideal then $B/J$ is a domain, and $A/f^{-1}(J)$ injects into it, therefore $A/f^{-1}(J)$ is also a domain and therefore $f^{-1}(J)$ is a prime ideal. □

LEMMA 9.2.4. *$R_{\mathfrak{p}}$ is a local ring with a maximal ideal extended from $\mathfrak{p}$.*

*Proof.* We will use the following simple observation: If $A$ is a local ring with a maximal ideal $\mathfrak{m}$ then any $x \notin \mathfrak{m}$ is not contained in a proper ideal and therefore is invertible. Elements in $\mathfrak{m}$ are of course not invertible. And the other way around, if $A^* \subset A$ is the set of invertible elements (units) and $\mathfrak{m} = A \setminus A^*$ happens to be an ideal of $A$ then $A$ is a local ring with a maximal ideal $\mathfrak{m}$, because any proper ideal does not intersect $A^*$.

Returning to $R_{\mathfrak{p}}$, let $\mathfrak{m}$ be the extension of the ideal $\mathfrak{p}$. This is a proper ideal by the previous proposition. But any element not in $\mathfrak{m}$ has form $r/s$ with $r, s \notin \mathfrak{p}$, which is obviously invertible in $R_{\mathfrak{p}}$. So $R_{\mathfrak{p}}$ is a local ring. □

## §9.3. **Spectrum and Nilradical.**

DEFINITION 9.3.1. The set of all prime ideals of the ring $R$ is called *spectrum* and denoted by $\operatorname{Spec} R$. For any homomorphism of rings $A \to B$ we have a pull-back map $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ defined as follows: $f^*(\mathfrak{p}) = f^{-1}(\mathfrak{p})$ for any prime ideal $\mathfrak{p} \subset B$.

PROPOSITION 9.3.2. *Let $R$ be a commutative ring. The intersection of all its prime ideals is equal to the set of nilpotent elements (called the nilradical) of $R$:*

$$\bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p} = \{x \in R \,|\, x^n = 0 \text{ for some } n > 0\}.$$

*Proof.* If $\mathfrak{p}$ is a prime ideal and $x^n = 0$ for some $n$ then $x^n \in \mathfrak{p}$ and therefore $x \in \mathfrak{p}$. Now suppose that $x$ is not nilpotent. Then

$$S = \{1, x, x^2, \dots\}$$

is a multiplicative system. Consider the localization $S^{-1}R$ and any maximal (and hence prime) ideal $I$ of it. Then $\mathfrak{p} = R \cap I$ is a prime ideal of $R$ that does not intersect $S$, and therefore does not contain $x$. □

## §9.4. **Going-up Theorem.**

THEOREM 9.4.1 (Going-up Theorem). *Let $A \subset B$ be rings and suppose that $B$ is integral over $A$. Then the pull-back map* $\operatorname{Spec} B \to \operatorname{Spec} A$ *is surjective.*

*Proof.* We have to show that for any prime ideal $\mathfrak{p} \subset A$, there exists a prime ideal $\mathfrak{q} \subset B$ such that

$$\mathfrak{p} = \mathfrak{q} \cap A.$$

Let $S \subset A$ be a complement of $\mathfrak{p}$. Localizing at $S$, we get a commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & S^{-1}B \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_{\mathfrak{p}} \end{array} \tag{14}$$

where the vertical arrows are inclusions. Notice that $S^{-1}B$ is integral over $A_{\mathfrak{p}}$: if $b \in B$ satisfies a monic equation

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0$$

then $b/s$ for $s \in S$ satisfies a monic equation

$$(b/s)^n + (a_1/s)(b/s)^{n-1} + \ldots + (a_n/s^n) = 0.$$

Suppose we can prove the theorem for $A_{\mathfrak{p}} \subset S^{-1}B$. Then there exists a prime ideal $J$ of $S^{-1}B$ such that $J \cap A_{\mathfrak{p}} = S^{-1}\mathfrak{p}$. Let $\mathfrak{q} = B \cap J$. We claim that $\mathfrak{q}$ restricts to $\mathfrak{p}$ in $A$. This follows from commutativity of the diagram (14) and the facts that $J$ restricts to $S^{-1}\mathfrak{p}$ in $A_{\mathfrak{p}}$ and $S^{-1}\mathfrak{p}$ restricts to $\mathfrak{p}$ in $A$ (by Prop. 9.2.3).

So we reduced to the case when $A$ is local with a maximal ideal $\mathfrak{m} = \mathfrak{p}$. Let $\mathfrak{m}' \subset B$ be any maximal ideal. We claim that $\mathfrak{m}' \cap A = \mathfrak{m}$. In any case, $\mathfrak{m}' \cap A \subset \mathfrak{m}$ because $A$ is local. We have a commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & B/\mathfrak{m}' \\ \uparrow & & \uparrow \\ A & \longrightarrow & A/(\mathfrak{m}' \cap A) \end{array}$$

where the vertical arrows are inclusions. Notice that $B/\mathfrak{m}'$ is a field integral over $A/(\mathfrak{m}' \cap A)$. But then $A/(\mathfrak{m}' \cap A)$ is a field (see the proof of Lemma 8.2.2 or Exercise 9 from the previous homework). So $\mathfrak{m}' \cap A$ is a maximal ideal, and therefore $\mathfrak{m}' \cap A = \mathfrak{m}$. □

EXAMPLE 9.4.2. Let $y = x^2$ and consider the embedding $f : \mathbb{C}[y] \hookrightarrow \mathbb{C}[x]$. Since $x$ satisfies the monic equation $T^2 - y = 0$, $\mathbb{C}[x]$ is integral over $\mathbb{C}[y]$ and hence the going-up theorem applies. What does it mean geometrically? There are two types of prime ideals of $\mathbb{C}[x]$: the zero ideal obviously restricts to the zero ideal of $\mathbb{C}[y]$. Any other ideal is maximal and has the

form $(x-a)$ for a fixed $a \in \mathbb{C}$. What does it restrict to? The ideal $(x-a)$ is the kernel of the homomorphism of $\mathbb{C}$-algebras

$$\mathbb{C}[x] \to \mathbb{C}, \quad x \mapsto a,$$

so its pull-back $f^{-1}(x-a)$ is the kernel of the homomorphism

$$\mathbb{C}[y] \hookrightarrow \mathbb{C}[x] \to \mathbb{C},$$

$$y \mapsto x^2 \mapsto a^2.$$

So $f^*(x-a) = (y-a^2)$, i.e. geometrically $f^*$ is just the map $\mathbb{A}^1_{\mathbb{C}} \to \mathbb{A}^1_{\mathbb{C}}$, $a \mapsto a^2$. So in this case the going-up theorem is simply saying that any complex number is a square.

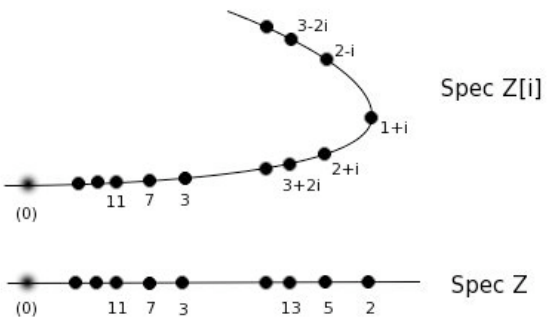
EXAMPLE 9.4.3. Consider the embedding $f : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$. Since $i$ satisfies the monic equation $T^2+1=0$, this is an integral extension. These rings are PIDs, and non-zero prime ideals correspond to primes in $\mathbb{Z}$ and in $\mathbb{Z}[i]$ (up-to association). So suppose $\gamma \in \mathbb{Z}[i]$ is prime and let $p \in \mathbb{Z}$ be a prime such that $(p) = (\gamma) \cap \mathbb{Z}$. We have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}/(p) & \hookrightarrow & \mathbb{Z}[i]/(p) \\ & \searrow & \downarrow \\ & & \mathbb{Z}[i]/(\gamma) \end{array}$$

Notice that the field extension $\mathbb{Z}/(p) \subset \mathbb{Z}[i]/(\gamma)$ is generated by the image of $i$ in $\mathbb{Z}[i]/(\gamma)$, and consequently has degree $1$ or $2$ depending on whether $-1$ is a square in $\mathbb{Z}/(p)$ or not. If $-1$ is not a square then the map $\mathbb{Z}[i]/(p) \to \mathbb{Z}[i]/(\gamma)$ is an isomorphism (as both sets have $p^2$ elements and this map is surjective). Therefore, in this case $(p) = (\gamma)$ and $p = \gamma$ up to association. If $-1$ is a square modulo $p$ then $\mathbb{Z}[i]/(\gamma)$ has $p$ elements, and therefore $|\gamma| = \sqrt{p}$ (draw a square in $\mathbb{Z}[i]$ with vector sides $\gamma$ and $i\gamma$). It follows that $\gamma\overline{\gamma} = p$. Since $\mathbb{Z}[i]$ is a PID, it follows that there are exactly two possibilities for $\gamma$, unless $\gamma$ and $\overline{\gamma}$ are associate, i.e. if $\gamma/\overline{\gamma}$ is a unit in $\mathbb{Z}[i]$. There are just $4$ units, $\pm 1$ and $\pm i$, and it is easy to see that $\gamma$ and $\overline{\gamma}$ are associate if and only if $\gamma = 1+i$ (up to association).

Finally, it is very easy to see (using the fact that $\mathbb{F}_p^*$ is cyclic) that $-1$ is not a square modulo $p$ if and only if $p \equiv 3 \mod 4$.

So the full picture of the pull-back map is as follows:



§9.5. **Exercises.**

In this worksheet, $k$ denotes a field and $R$ denotes a commutative ring. Do not assume that $k$ is algebraically closed unless otherwise stated.

**1.** Let $S \subset R$ be a multiplicative system. Consider the covariant functor $\mathbf{Rings} \to \mathbf{Sets}$ that sends a ring $A$ to the set of all homomorphisms $f : R \to A$ such that $f(s)$ is a unit for any $s \in S$ (describe its action of homomorphisms $A \to A'$ yourself). Show that this functor is representable.

**2.** Show that a ring $A$ is local if and only if its non-invertible elements form an ideal.

**3.** Let $f : A \to B$ be a homomorphism of rings. If $I$ is an ideal of $B$ then we define its contraction as $I^c = f^{-1}(I)$. If $I$ is an ideal of $A$ then we define its extension as $I^e = Bf(I)$. (a) Is it true that any ideal of $B$ is extended? (b) Is it true that $(I^c)^e = I$ for any ideal $I$ of $B$? (c) Show that the maps $I \to I^e$ and $I \to I^c$ induce a bijection between the set of contracted ideals in $A$ and the set of extended ideals in $B$.

**4.** For any ideal $I$ of $R$, let $V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \,|\, I \subset \mathfrak{p}\}$. (a) Show that $\operatorname{Spec} R$ satisfies all axioms of a topological space with closed subsets $V(I)$. This topology is called *Zariski topology*. (b) Show that the pull-back $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is continuous in Zariski topology.

**5.** Let $S \subset R$ be a multiplicative subset and let $f : R \to S^{-1}R$ be a canonical homomorphism. (a) Show that the pull-back map $f^* \operatorname{Spec} S^{-1}R \to \operatorname{Spec} R$ is injective. (b) Let $I \subset R$ be an ideal. Show that $S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$.

**6.** Let $\mathfrak{p} \subset R$ be a prime ideal. Show that the image of $\operatorname{Spec} R_{\mathfrak{p}}$ in $\operatorname{Spec} R$ is equal to the intersection of all open subsets in $\operatorname{Spec} R$ that contain a point $\mathfrak{p}$.

**7.** Let $\Sigma$ be the set of all multiplicative subsets of $R$. Show that $\Sigma$ contains maximal (by inclusion) subsets and that $S \in \Sigma$ is maximal if and only if $R \setminus S$ is a minimal prime ideal.

**8.** Describe (a) $\operatorname{Spec} \mathbb{Z}/n\mathbb{Z}$; (b) $\operatorname{Spec} \mathbb{Z}_5$ (5-adic numbers).

**9.** Let $I \subset R$ be an ideal. Show that

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} R \\ I \subset \mathfrak{p}}} \mathfrak{p}.$$

**10.** Let $\sqrt{0} \subset R$ be the nil-radical. Show that the canonical pull-back map $\operatorname{Spec} R/\sqrt{0} \to \operatorname{Spec} R$ is a homeomorphism (first show that it is a bijection of sets).

**11.** Suppose $R$ is a direct product of rings $R_1 \times \ldots \times R_k$. Show that $\operatorname{Spec} R$ is homeomorphic to the disjoint union of spectra $\operatorname{Spec} R_1, \ldots, \operatorname{Spec} R_k$.

**12.** (a) Show that the intersection of closed subsets $\cap_\alpha V(I_\alpha)$ of $\operatorname{Spec} R$ is empty if and only if $\sum_\alpha I_\alpha = R$. (b) Show that $\operatorname{Spec} R$ is quasi-compact, i.e. any open covering of $\operatorname{Spec} R$ has a finite sub-covering.

**13.** Let $f : A \to B$ be a homomorphism of rings. (a) Show that the pull-back $f^* : \operatorname{MaxSpec} B \to \operatorname{MaxSpec} A$ is not always well-defined. (b) If $A$ and $B$ are finitely generated $k$-algebras then the pull-back for $\operatorname{MaxSpec}$ is well-defined (do not assume that $k$ is algebraically closed, although it helps to consider this case first).

**14.** Let $J, I_1, \ldots, I_r$ be ideals of $R$ such that $J \subset I_1 \cup \ldots \cup I_r$. Show that $J$ is in fact contained in one of the ideals $I_k$ if any of the following conditions are satisfied. (a) $r = 2$. (b) All ideals $I_1, \ldots, I_r$ are prime (Hint: prove the contrapositive statement by induction on $r$).

**15.** Let $J, I_1, \ldots, I_r$ be ideals of $R$ such that $J \subset I_1 \cup \ldots \cup I_r$. Show that $J$ is in fact contained in one of the ideals $I_k$ if any of the following conditions are satisfied. (a) At most two of the ideals $I_1, \ldots, I_r$ are not prime. (b) $R$ contains an infinite field.

## §10. Geometry and Commutative Algebra - II

### §10.1. Localization as a functor $\mathbf{Mod}_R \to \mathbf{Mod}_{S^{-1}R}$.

Localization of rings $R \mapsto S^{-1}R$ can be extended to localization of modules.

Definition 10.1.1. Let $M$ be an $R$-module. We define $S^{-1}M$ as the set of equivalence classes of fractions $m/s$, where $m \in M$, $s \in S$, such that two fractions $m/s$ and $m'/s'$ are considered equivalent if there exists $t \in S$ such that

$$t(s'm - sm') = 0.$$

(Note that even if $R$ is a domain, $M$ can have elements annihilated by some $t \in S$, so the standard cross-multipication definition has to be modified to include $t$.) We make $S^{-1}M$ into an $S^{-1}R$-module by declaring that $r/s \in S^{-1}R$ acts on $m/t \in S^{-1}M$ by sending it to $(rm)/(st)$.

Notation 10.1.2. If $\mathfrak{p} \in \operatorname{Spec} R$ and $S = R \setminus \mathfrak{p}$ then $S^{-1}M$ is denoted by $M_{\mathfrak{p}}$.

What is the geometry behind this: rings correspond to spaces, modules correspond to vector bundles (and more general quasi-coherent sheaves): explain how (sections). Vector bundle is a "local concept" (we can restrict vector bundles and their sections to open subsets) and localization makes this procedure algebraic.

Lemma 10.1.3. *Localization is a functor*

$$S^{-1}\cdot : \mathbf{Mod}_R \to \mathbf{Mod}_{S^{-1}R}.$$

*In fact, localization of a module is a special case of extension of scalars:*

$$S^{-1}M \simeq S^{-1}R \otimes_R M$$

*and functors $S^{-1}\cdot$ and $S^{-1}R \otimes \cdot$ are naturally isomorphic.*

*Proof.* Explain how $S^{-1}$ acts on morphisms. For an isomorphism, we have a bilinear map of $R$ modules

$$S^{-1}R \times M \to S^{-1}M,$$

which induces an (obviously surjective) map of $R$-modules

$$\psi : S^{-1}R \otimes_R M \to S^{-1}M,$$

Why is it injective? Any element of $S^{-1}R \otimes_R M$ has the form

$$\sum_i (r_i/s_i) \otimes m_i = \sum_i (t_i r_i/s) \otimes m_i = \sum_i (1/s) \otimes t_i r_i m_i = (1/s) \otimes m,$$

where $s = \prod_i s_i$. If $0 = \psi((1/s) \otimes m) = (m/s)$ then $tm = 0$ for some $t \in S$. But then

$$(1/s) \otimes m = (t/ts) \otimes m = (1/ts) \otimes tm = 0.$$

□

The localization functor has one very important and unusual property:

LEMMA 10.1.4. *Localization is an exact functor.*

*Proof.* We have already used that tensoring with anything is a right-exact functor. So we only have to check that if $i : M \hookrightarrow N$ is an inclusion then $S^{-1}i : S^{-1}M \to S^{-1}N$ is an inclusion as well. Suppose $S^{-1}i(m/s) = i(m)/s = 0$ in $S^{-1}N$. Then $ti(m) = i(tm) = 0$ for some $t \in S$. But then $tm = 0$ in $M$ and therefore $m/s = 0$ in $S^{-1}M$. □

We see that if $M$ is a submodule of $N$ then we can view $S^{-1}M$ as a submodule of $S^{-1}N$.

§10.2. **Nakayama's Lemma.** We are trying to translating geometric ideas into algebra and vice versa by drawing not very rigorous but very useful parallels, and also by developing the language of algebraic geomtry where these parallels become rigorous.

Vector bundles on a space correspond to modules of a ring. In fact, locally a vector bundle is trivial, and so a vector bundle corresponds to a free module.

More precisely, the category of vector bundles is not Abelian (roughly speaking, the category is Abelian if objects and morphisms can be added, kernels and cokernels exist and satisfy the first isomorphism theorem, direct sums exists, and a bunch of other formal properties). Te problem here is that cokernels dont' exist. We can try to extend the category of vector bundles to a category of *coherent sheaves*, in which cokernels always exist.

What will happen if we start with a category of free modules of finite rank over a ring $R$ and extend it to include all cokernels? We will get the category of finitely presented modules. If the ring is Noetherian, we will get the category of finitely generated modules (which in this case will be an Abelian category).

One often needs to check that a bunch of sections $s_1, \dots, s_n$ of a vector bundle is its basis. For example, any tangent vector field can be written locally as

$$\sum a_i(x_1, \dots, x_n) \frac{\partial}{\partial x_i},$$

i.e. $\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_1}$ is a basis of a tangent bundle (locally in the chart where the coordinates $\{x_i\}$ are defined). In general, there is a simple and useful trick for this: if $s_1(x_0), \dots, s_n(x_0)$ is a basis of a fiber of a vector bundle at a point $x_0$ then sections form a basis in the neighborhood of this point. What is an algebraic analogue of this principle?

Instead of the space $X$, we take a ring $R$. Instead of a vector bundle, we take a *finitely generated* module $M$. We also have a bunch of elements $s_1, \dots, s_n$. What is the analogue of the statement that they "generate the fiber of a vector bundle at $x_0 \in X$"? A point of $X$ corresponds to a maximal ideal $\mathfrak{m} \subset R$. A section $s$ that vanishes at a point $x_0$ can be written as

$fs'$, where $f$ is a function such that $f(x_0) = 0$. So "a fiber at $x_0$" corresponds to $M/\mathfrak{m}M$. So we assume that cosets of $s_1, \ldots, s_n$ in $M/\mathfrak{m}M$ generate this module, i.e. that $M = Rs_1 + \ldots + Rs_n + \mathfrak{m}M$. Finally, we are not really claiming that $s_1, \ldots, s_n$ should generate $M$ but rather that they will generate $M$ "locally". So we are going to localize $R$ at $\mathfrak{m}$, or even just assume from the beginning that $R$ is local with a maximal ideal $\mathfrak{m}$. So we get

LEMMA 10.2.1 (Nakayama's Lemma). *Let $R$ be a local ring with a maximal ideal $\mathfrak{m}$ and let $M$ be a finitely generated $R$-module with elements $s_1, \ldots, s_n$. If this elements generate $M$ modulo $\mathfrak{m}M$ then in fact they generate $M$.*

Here is a more eloquent formulation of the same idea:

LEMMA 10.2.2 (Nakayama's Lemma). *Let $R$ be a local ring with a maximal ideal $\mathfrak{m}$ and let $M$ be a finitely generated $R$-module. If $\mathfrak{m}M = M$ then $M = 0$.*

To deduce the previous version of Nakayama, let $N$ be a submodule of $M$ generated by $s_1, \ldots, s_n$. Then we are given that $M = N + \mathfrak{m}M$, i.e. that $M/N = \mathfrak{m}(M/N)$. We deduce that $M/N = 0$, i.e. that $M = N$.

Remember a "determinant" trick we used to show that $x \in B$ is integral over a subring $A \subset B$ if and only if $x$ is contained in a finitely generated $A$-submodule of $B$? The proof of Nakayama's lemma is another application of the same idea.

*Proof.* We will prove a slightly more general result. Let $R$ be any ring and let $M$ be a finitely generated $R$-module. If $I$ is an ideal contained in all maximal ideals and $IM = M$ then $M = 0$.

Let $m_1, \ldots, m_k$ be generators of $M$. Then we have

$$m_i = \sum a_{ij} m_j,$$

where $a_{ij} \in I$. Then

$$\sum_j (\delta_{ij} - a_{ij}) m_j = 0$$

for any $i$. Multiplying by the adjoint matrix, we see that

$$a m_j = 0$$

for any $j$, where $a = \det(\delta_{ij} - a_{ij})$. Notice that $a$ can be written as $1 + x$, where $x \in I$. We claim that $a$ is invertible. If not, then it belongs to some ideal and therefore belongs to some maximal ideal $\mathfrak{m} \subset R$. But $x$ also belongs to this ideal, and therefore $1 \in \mathfrak{m}$, a contradiction. It follows that $a$ is invertible and therefore

$$m_j = a^{-1}(a m_j) = 0$$

for any $j$, i.e. $M = 0$. □

§10.3. Spec **and** MaxSpec**. Irreducible Algebraic Sets.** Let $k = \bar{k}$ and let $R$ be the algebra of polynomials in $n$ variables over $k$. $R$ is the ring of functions on the affine space $\mathbb{A}^n_k$. Weak Nullstellensatz identifies points of $\mathbb{A}^n$ with maximal ideals in $R$ (of polynomials that vanish at these points). We have a Zariski topology on $\mathbb{A}^n$ with closed sets

$$V(I) = \{x \in \mathbb{A}^n \mid f(x) = 0 \text{ for any } f \in I\}$$

for any ideal $I \subset R$ (in fact strong Nullstellensatz gives a bijection between closed subsets of $\mathbb{A}^n$ and radical ideals of $R$). In the language of $\mathrm{MaxSpec}$, the Zariski topology looks as follows:

$$V(I) = \{\mathfrak{m} \in \operatorname{MaxSpec} R \,|\, I \subset \mathfrak{m}\}.$$

So we see that the Zariski topology on $\mathbb{A}^n$ is the restriction of Zariski topology on $\operatorname{Spec} R$, which is defined in exactly the same way. But now the question is, how to locate other points of $\operatorname{Spec} R$ in $\mathbb{A}^n$?

EXAMPLE 10.3.1. Let $R = k[x]$. The only prime ideal in $R$ that is not maximal is $(0)$, i.e.

$$\operatorname{Spec} R = \mathbb{A}^1_k \cup \eta, \text{ where } \eta = (0)$$

in this case. This point $\eta$ has a remarkable property: it is not closed! In fact, the only ideal contained in $(0)$ is $(0)$ itself, and so

$$\bar{\eta} = V(0) = \operatorname{Spec} R!$$

Draw a picture of a fuzzy point $\eta$.

EXAMPLE 10.3.2. Let $R = k[x, y]$. The prime ideals of $R$ are

- maximal ideals $(x - a, y - b)$;
- ideals $(f)$, where $f \in k[x, y]$ is an irreducible polynomial;
- $(0)$.

The corresponding closed algebraic sets are

- points $(a, b) \in \mathbb{A}^2$;
- curves $f = 0$, where $f \in k[x, y]$ is an irreducible polynomial;
- $\mathbb{A}^2$.

Draw a picture of $\operatorname{Spec} k[x, y]$.

Let's consider the general case.

DEFINITION 10.3.3. A subset of a topological space is called *irreducible* if it is not a union of two proper closed subsets.

What are the irreducible subsets of $\mathbb{R}^n$ in the usual Euclidean topology? Not so in Zariski topology!

LEMMA 10.3.4. *Irreducible subsets of $\mathbb{A}^n$ bijectively $Y \to I(Y)$ correspond to prime ideals of $R$. For any $\mathfrak{p} \in \operatorname{Spec} R$,*

$$\overline{\mathfrak{p}} \cap \operatorname{MaxSpec} R = V(\mathfrak{p}).$$

*Proof.* Suppose $Y \subset \mathbb{A}^n$ is a reducible subset, $Y = Y_1 \cup Y_2 = V(I_1) \cup V(I_2)$. Then there exist $f \in I_1$ and $g \in I_2$ that do not vanish identically on $Y$, i.e. they do not belong to $I(Y)$. However, clearly $fg \in I(Y)$. This shows that $I(Y)$ is not prime.

If $I = I(Y)$ is not prime then take $f, g \in R \setminus I$ such that $fg \in I$. Then $f$ or $g$ vanishes at any point of $Y$, i.e. $Y$ can be decomposed as

$$(Y \cap V(f)) \cup (Y \cap V(g))$$

The last part is obvious. □

This gives us another way of thinking about $A^n$: this is the set of *closed points* in $\operatorname{Spec} R$.

DEFINITION 10.3.5. Let $Y \subset \mathbb{A}^n$ be a closed algebraic subset. Maximal (by inclusion) irreducible subsets of $Y$ are called its *irreducible components*.

THEOREM 10.3.6. *Let $Y \subset \mathbb{A}^n_k$ be a Zariski closed subset. Then $Y$ has only finitely many irreducible components $Y_1, \ldots, Y_n$ and we have*

$$Y = Y_1 \cup \ldots \cup Y_n.$$

*Proof.* It suffices to prove that $Y$ can be written as a finite union of irreducible subsets $Z_1, \ldots, Z_r$. Indeed, by throwing away subsets contained in other subsets we will reduce to the case $Z_i \not\subset Z_j$ for $i \neq j$. If $Z \subset Y$ is any subset then $Z = (Z \cap Z_1) \cup \ldots (Z \cap Z_r)$, and so if $Z$ is irreducible then it is contained in one of the $Z_i$'s and therefore $Z_i$'s are exactly irreducible components of $Y$.

Let's prove the claim. If $Y$ is irreducible then there is nothing to do. If $Y = Y_1 \cup Y_2$ then we can start breaking $Y_1$ and $Y_2$ into irreducible components. We claim that this process sooner or later stops. If it does not then we will produce the chain of closed subsets

$$Y = Y^1 \supset Y^2 \supset Y^3 \supset \ldots$$

where $Y^i \neq Y^{i+1}$. But then

$$I(Y^1) \subset I(Y^2) \subset I(Y^3) \subset \ldots$$

is an increasing chain of ideals, which contradicts the Hilbert basis theorem (the ring of polynomials is Noetherian). □

§10.4. **Morphisms of Algebraic Sets.** Let $k = \bar{k}$ be an algebraically closed field. If $Y \subset \mathbb{A}^n_k$ is a closed algebraic set then we have the algebra of "restrictions of polynomial functions"

$$\mathcal{O}(Y) = k[x_1, \ldots, x_n]/I(Y).$$

Notice that $Y$ is irreducible if and only if $\mathcal{O}(Y)$ is a domain.

Now suppose we have two algebraic sets,

$$Y_1 \subset \mathbb{A}^n_{x_1,\ldots,x_n} \text{ and } Y_1 \subset \mathbb{A}^m_{y_1,\ldots,y_m}$$

(subscripts indicate variables). What are the "maps" from $Y_1$ to $Y_2$?

DEFINITION 10.4.1. A map $\alpha : Y_1 \to Y_2$ is called a *morphism* if $\alpha$ is a restriction of the polynomial map

$$\mathbb{A}^n_{x_1,\ldots,x_n} \to \mathbb{A}^m_{y_1,\ldots,y_m}, \quad y_i = f_i(x_1, \ldots, x_n),$$

i.e. if there exists $m$ polynomials $f_1, \ldots, f_m$ in variables $x_1, \ldots, x_n$ such that

$$\alpha(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots f_1(a_1, \ldots, a_n))$$

for any point $(a_1, \ldots, a_n) \in Y_1$.

EXAMPLE 10.4.2. The map

$$t \mapsto (t^2, t^3)$$

is a morphism from $\mathbb{A}^1$ to the cusp $(x^3 = y^2) \subset \mathbb{A}^2$.

EXAMPLE 10.4.3. We have a map from $\mathbb{A}^1_t$ to the parabola $X = \{y = x^2\} \subset \mathbb{A}^2$, $t \mapsto (t, t^2)$ and the map $X \to \mathbb{A}^1$ given by $(x, y) \mapsto x$. This maps are inverses of each other.

For any morphism $\alpha: Y_1 \to Y_2$, we can define a *pull-back map*

$$\alpha^*: \mathcal{O}(Y_2) \to \mathcal{O}(Y_1).$$

Let $f \in \mathcal{O}(Y_2)$ and let $a \in Y_1$ then we simply define

$$(\alpha^* f)(a) = f(\alpha(a)).$$

To show that $\alpha^* f \in \mathcal{O}(Y_1)$, we have to show that it is a restriction of the polynomial function on $\mathbb{A}^n$. But indeed, let $f$ be a restriction of the polynomial $\bar{f} \in k[y_1, \dots, y_m]$. Then $\alpha^*(f)$ is the restriction of the function

$$\bar{f}(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$

which is obviously a polynomial.

EXAMPLE 10.4.4. For the map

$$\alpha: \mathbb{A}^1 \to X = (x^3 = y^2) \subset \mathbb{A}^2, \quad t \mapsto (t^2, t^3),$$

we have $\mathcal{O}(X) = k[x, y]/(x^3 - y^2)$, and

$$\alpha^*: k[x, y]/(x^3 - y^2) \to k[t], \quad x \mapsto t^2,\ y \mapsto t^3.$$

EXAMPLE 10.4.5. The bijections between $\mathbb{A}^1$ and the parabola $X = \{y = x^2\} \subset \mathbb{A}^2$ discussed above induce isomorphisms

$$\mathcal{O}(X) = k[x, y]/(y - x^2) \simeq k[t] = \mathcal{O}(\mathbb{A}^1), \quad (x \mapsto t,\ y \mapsto t^2), \quad (t \mapsto x).$$

THEOREM 10.4.6. *We have a contravariant functor $Y \mapsto \mathcal{O}(Y)$ from the category of closed algebraic sets to the category of finitely generated $k$-algebras without nilpotents. This functor is an equivalence of categories.*

*Proof.* Since $I(Y)$ is a radical ideal, $\mathcal{O}(Y)$ has no nilpotents. It is finitely generated as the quotient of a polynomial algebra in finitely many variables. It is clear that $\alpha^*$ is a homomorphism of $k$-algebras. So we have our functor.

Why is it an equivalence of categories? We have to check two things. Firstly, we have to check that it is essentially surjective. If $R$ is a finitely generated $k$-algebra without nilpotents then we can write

$$R = k[x_1, \dots, x_n]/I,$$

where $I$ is a radical ideal. Let

$$X = V(I) \subset \mathbb{A}^n.$$

By Nullstellensatz, $I = I(X)$. So any finitely generated algebra without nilpotents is isomorphic to one of the form $\mathcal{O}(X)$.

Secondly, we have to check that it is fully faithful, i.e.

$$\mathbf{Mor}(Y_1, Y_2) = \mathrm{Hom}(\mathcal{O}(Y_2), \mathcal{O}(Y_1)).$$

If $\alpha: Y_1 \to Y_2$ is a morphism and

$$\alpha(a_1, \dots, a_n) = (b_1, \dots, b_m)$$

for some $(a_1, \dots, a_n) \in Y_1$ Then $b_i = \alpha^*(y_i)(a_1, \dots, a_n)$. So we can recover $\alpha$ from $\alpha^*$. Finally, let

$$F: \mathcal{O}(Y_2) \to \mathcal{O}(Y_1)$$

be a homomorphism. We have to realize it as a pull-back homomorphism for some morphism of algebraic sets. For each $i = 1, \dots, m$ choose a representative $f_i \in k[x_1, \dots, x_n]$ of a coset $F(y_i)$ and consider a morphism

$$\alpha : \mathbb{A}^n \to \mathbb{A}^m$$

given by these polynomials. We claim that $\alpha(Y_1) \subset Y_2$. It suffices to check that any polynomial $f \in I(Y_2)$ vanishes on $\alpha(Y_1)$. In other words, the claim is that $f(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ vanishes on $Y_1$. But this polynomial is equal to $F(f)$, which belongs to $I(Y_1)$. □

§10.5. **Dominant morphisms.** Let's translate some geometry into algebra.

DEFINITION 10.5.1. A morphism $\alpha : Y_1 \to Y_2$ of algebraic sets is called *dominant* if its image is Zariski dense in $Y_2$.

EXAMPLE 10.5.2. Consider a projection from the hyperbola $xy = 1$ to the $x$-axis. The image misses only $0 \in \mathbb{A}^1$, and so this map is dominant. What can we say about the pull-back homomorphism? It is

$$k[x] \to k[x, y]/(xy = 1) = k[x, \frac{1}{x}], \quad x \mapsto x.$$

Notice that it is injective. This is not a coincidence.

PROPOSITION 10.5.3. *$\alpha : Y_1 \to Y_2$ is dominant if and only if $\alpha^*$ is injective.*

*Proof.* Suppose $\alpha$ is dominant. Let $f \in \operatorname{Ker} \alpha^*$. Then $f(\alpha(a)) = 0$ for any $a \in Y_1$, i.e. $\alpha$ maps $Y_1$ to a closed subset $V(f) \cap Y_2$. But $\overline{\alpha(Y_1)} = Y_2$, therefore $V(f) \cap Y_2 = Y_2$, i.e. $f$ vanishes on $Y_2$ identically, i.e. $f = 0$.

Suppose $\alpha$ is not dominant. Then $\overline{\alpha(Y_1)}$ is a proper closed subset of $Y_2$, and therefore there exists $f \in \mathcal{O}(Y_2)$, $f \neq 0$, such that $\overline{\alpha(Y_1)} \subset V(f)$. But then $\alpha^*(f) = 0$, i.e. $\operatorname{Ker} \alpha^* \neq 0$. □

§10.6. **Finite Morphisms.** Now let's translate some algebra into geometry.

DEFINITION 10.6.1. A morphism of algebraic sets $X \to Y$ is called *finite* if $\mathcal{O}(X)$ is integrally closed over $\mathcal{O}(Y)$ by the pull-back map.

THEOREM 10.6.2. *Suppose $\alpha : X \to Y$ is a dominant finite morphism. Then $\alpha$ is surjective and has finite fibers.*

EXAMPLE 10.6.3. Notice that this gives a beautiful (and very useful) way to reformulate Noether's normalization lemma: any affine algebraic set admits a finite morphism to $\mathbb{A}^n$ for some $n$.

*Proof.* Let $A = \mathcal{O}(X)$ and let $B = \mathcal{O}(Y)$. By Lemma 10.5.3, $B \subset A$ and $A$ is integral over $B$. Let $x \in Y$. It corresponds to a maximal ideal $\mathfrak{m} \subset B$. To show that $\alpha$ is surjective, we have to check that there exists a maximal ideal $\mathfrak{n} \subset A$ such that $\mathfrak{n} \cap B = \mathfrak{m}$ and to show that $\alpha$ has finite fibers, we have to check that there are finitely many possible $\mathfrak{n}$'s. By the going-up theorem, we can find a prime ideal $\mathfrak{p} \subset A$ such that $\mathfrak{p} \cap B = \mathfrak{m}$. But then $A/\mathfrak{p}$ is a domain integral over a field $k = B/\mathfrak{m}$, so as we have seen many times already $A/\mathfrak{p} = k$ (here we are using that $k$ is algebraically closed, otherwise we will get a finite extension of $k$), and therefore $\mathfrak{p}$ is in fact a maximal ideal. Moreover, we see that there is a bijection between $\mathfrak{n}$'s and maximal ideals

of the algebra $A/A\mathfrak{m}$. The latter algebra is integral over $B/\mathfrak{m} = k$, and so is a finitely generated $k$-module, i.e. a finite-dimensional vector space. In particular, $A/A\mathfrak{m}$ is Artinian, i.e. satisfies descending chain condition for modules. So it is enough to prove the following more general lemma. □

LEMMA 10.6.4. *Any Artinian ring $R$ has the following properties:*

- *Any prime ideal of $R$ is maximal.*
- *$R$ has only finitely many maximal ideals.*

*Proof.* For the first statement, if $\mathfrak{p} \subset R$ is a prime ideal then $R/\mathfrak{p}$ is an Artinian domain, which must be a field: for any $x \in R/\mathfrak{p}$, the sequence

$$(x) \supset (x^2) \supset (x^3) \supset \dots$$

stabilizes, and therefore $x^n = x^{n+1}y$ for some $n$, $y \in R/\mathfrak{p}$, but this implies $1 = xy$. So $\mathfrak{p}$ is maximal.

For the second statement, consider the set of finite intersections of maximal ideals. By d.c.c, this set has the minimal element, i.e. there exist maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_r \subset R$ such that

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$$

for any maximal ideal $\mathfrak{m}$, in particular

$$\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r \subset \mathfrak{m}.$$

We claim that this implies that $\mathfrak{m} = \mathfrak{m}_i$ for some $i$. If not, then each $\mathfrak{m}_i$ contains $x_i$ such that $x_i \notin \mathfrak{m}$. But then

$$x_1 \dots x_r \in \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r \subset \mathfrak{m},$$

and since $\mathfrak{m}$ is prime, one of the $x_i$'s is contained in $\mathfrak{m}$. □

§10.7. **Exercises.**

In this worksheet $R$ is a ring and $k = \bar{k}$ is an algebraically closed field.

**1.** Let $f, g \in k[x_1, \dots, x_n]$ be polynomials such that $f$ is irreducible and $V(f) \subset V(g)$. Show that $f$ divides $g$.

**2.** Let $\alpha : \mathbb{A}^2 \to \mathbb{A}^2$ be a morphism given by polynomials $f$ and $g$ in $k[x, y]$. (a) Show that if $\alpha$ is an isomorphism then the polynomial

$$\det \begin{bmatrix} \frac{\partial f(x,y)}{\partial x} & \frac{\partial g(x,y)}{\partial x} \\ \frac{\partial f(x,y)}{\partial y} & \frac{\partial g(x,y)}{\partial y} \end{bmatrix}$$

is a nonzero constant (the converse of this is a famous open problem). (b) Give an example when $\alpha$ is an isomorphism but polynomials $f, g$ are not both linear polynomials.

**3.** Let $X \subset \mathbb{A}^2$ be defined by equations $x^2 + y^2 = 1$ and $x = 1$. Is it true that $I(X) = (f, g)$?

**4.** (a) Let $X \subset \mathbb{A}^2$ be a cuspidal cubic $x^2 = y^3$. Let $f : \mathbb{A}^1 \to X$ be defined by formulas $t \mapsto (t^3, t^2)$. Is it an isomorphism? (b) Is a hyperbola $xy = 1$ isomorphic to $\mathbb{A}^1$?

**5.** Consider the morphism $\mathbb{A}^2 \to \mathbb{A}^2$ defined by formulas $(x, y) \mapsto (x, xy)$. Is the image Zariski closed? Zariski open? Zariski dense?

**6.** Show that the category of irreducible algebraic sets and morphisms between them is equivalent to the category of finitely generated $k$-algebras without zero-divisors and homomorphisms between them.

**7.** Consider the morphism $\alpha : \mathbb{A}^1 \to \mathbb{A}^n$ given by $t \mapsto (t, t^2, \dots, t^n)$. Show that $\alpha$ induces an isomorphism between $\mathbb{A}^1$ and $V(I)$, where $I$ is generated by $2 \times 2$ minors of the following matrix

$$\begin{bmatrix} 1 & x_1 & x_2 & \dots x_{n-1} \\ x_1 & x_2 & x_3 & \dots x_n \end{bmatrix}$$

In the problems 8–11, let $S$ be a multiplicative system in $R$.

**8.** Let $M_1$ and $M_2$ be submodules of an $R$-module $N$. Show that

$$(a) \qquad (S^{-1}M_1) + (S^{-1}M_2) = S^{-1}(M_1 + M_2);$$

$$(b) \qquad (S^{-1}M_1) \cap (S^{-1}M_2) = S^{-1}(M_1 \cap M_2);$$

$$(c) \qquad \text{if } M_1 \supset M_2 \text{ then} \quad S^{-1}(M_1/M_2) \simeq (S^{-1}M_1)/(S^{-1}M_2).$$

**9.** Let $M$ be a finitely generated $R$-module. Let $\operatorname{Ann} M = \{r \in R \,|\, rM = 0\}$. Show that

$$S^{-1}(\operatorname{Ann} M) \simeq \operatorname{Ann}(S^{-1}M).$$

**10.** Let $M_1$ and $M_2$ be $R$-modules. Show that

$$S^{-1}(M_1 \otimes_R M_2) \simeq (S^{-1}M_1) \otimes_{S^{-1}R} (S^{-1}M_2).$$

**11.** Show that the nilradical of $S^{-1}R$ is isomorphic to the localization of the nilradical of $R$.

**12.** (a) Let $M$ be an $R$-module. Show that $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{m} \subset R$. (b) The ring is called *reduced* if its nilradical is trivial. Show that the ring $R$ is reduced if and only if $R_{\mathfrak{p}}$ s reduced for any prime ideal $\mathfrak{p} \subset R$.

**13.** Let $R$ be an integral domain. For any $R$-module $M$, let

$$T(M) = \{x \in M \,|\, rx = 0 \text{ for some } r \in R\}$$

be the torsion submodule of $M$. (a) Show that $M \to T(M)$ is a left-exact functor $\mathbf{Mod}_R \to \mathbf{Mod}_R$. (b) Show that $T(M) = 0$ if and only if $T(M)_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{p} \subset R$.

**14.** Let $R$ be a local Noetherian ring with a maximal ideal $\mathfrak{m}$. Show that

$$\bigcap_{n \geq 1} \mathfrak{m}^n = 0.$$

**15.** Show that the Nakayama's lemma fails if the module $M$ is not assumed to be finitely generated.

**16.** Let $M$ and $N$ be finitely generated modules over a local ring $R$. Show that if $M \otimes_R N = 0$ then $M = 0$ or $N = 0$.

**17.** For any $f \in R$, let $D(f) \subset \operatorname{Spec} R$ be the complement of the closed set $V(f)$. (a) Show that sets $D(f)$ form a base of Zariski topology, i.e. any Zariski open subset of $\operatorname{Spec} R$ can be expressed as a union of open sets of the form $D(f)$. (b) Show that if $D(f) = D(g)$ then $R[1/f] \simeq R[1/g]$.

**18.** Let $x, y \in \operatorname{Spec} R$. (a) Show that there exists either a neighborhood of $x$ that does not contain $y$ or a neighborhood of $y$ that does not contain $x$.

(b) Show that the nilradical of $R$ is a prime ideal if and only if $\operatorname{Spec} R$ contains a "generic point" $\eta$ such that $\bar{\eta} = \operatorname{Spec} R$.

**19.** For any $\mathfrak{p} \in \operatorname{Spec} R$, let $k(\mathfrak{p})$ be the quotient field of $R/\mathfrak{p}$. This field is called the residue field at $\mathfrak{p}$. (a) Show that

$$k(\mathfrak{p}) \simeq R_p/\mathfrak{p}R_{\mathfrak{p}}.$$

(b) Let $M$ be a finitely-generated $R$-module. The $k(\mathfrak{p})$-vector space

$$M \otimes_R k(\mathfrak{p})$$

is called *the fiber* of $M$ at $\mathfrak{p}$. Show that if $M \otimes_R k(\mathfrak{p}) = 0$ for any $\mathfrak{p} \in \operatorname{Spec} R$ then $M = 0$. (c) Let $R = \mathbb{Z}$ and let $M$ be a finitely generated Abelian group. Compute all fibers of $M$ on $\operatorname{Spec} Z$ and verify (b) in this case.

## §11. Representation Theory of Finite Groups

§11.1. **Representations of Finite Groups.** Let $G$ be a group and let $k$ be a field. The goal of representation theory is to add dynamics to a static definition of an abstract group by looking at its various matrix realizations.

Definition 11.1.1. A *representation* of $G$ is a homomorphism

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

where $V$ is a $k$-vector space. A representation is called *faithful* if $\rho$ is injective. It is called trivial if $\rho(G) = \{e\}$.

There are many ways to rephrase the definition. For example, a group $G$ will act on $V$ by a formula

$$g \cdot v = \rho(g)v, \quad g \in G,\ v \in V,$$

and this action is linear, i.e. any $g \in G$ acts on $V$ by linear operators. It is clear that any linear action of $G$ on $V$ is given by some representation.

We will only consider the case when $G$ is a finite group and $V$ is a finite-dimensional vector space. Very often one has interesting infinite dimensional representations: for example if the group $G$ acts on the space $X$ then it in fact acts linearly on its space of functions by a formula

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

The space of functions is usually infinite-dimensional. But for finite groups we won't loose much by concentrating on finite-dimensional representations.

Example 11.1.2. The symmetric group $S_n$ acts linearly on $k^n$ by permuting $n$ basis vectors. The corresponding representation $S_n \to \mathrm{GL}_n(k)$ is faithful and any $\sigma \in S_n$ is represented by a permutation matrix. This representation can be used to define the sign of a permutation:

$$\operatorname{sgn}(\sigma) = \det \rho(\sigma).$$

Since $\rho$ is a homomorphism $S_n \to \mathrm{GL}_n(k)$, and $\det$ is a homomorphism $\mathrm{GL}_n(k) \to k^*$, we see that $\operatorname{sgn}$ is a homomorphism $S_n \to k^*$. One can quickly check that $\operatorname{sgn}$ is equal to $(-1)^a$, where $a$ is a number of transpositions needed to write $\sigma$. This is the usual definition of the sign, but then one has to work to show that it is well-defined, i.e. does not depend on how we write a permutation as a product of transpositions.

EXAMPLE 11.1.3. Many groups are described as groups of symmetries of geometric objects, in which case one often has a representation. For example, the dihedral group $D_n$ is the group of symmetries of a regular $n$-gon. Choosing a cartesian coordinate system with the origin in the center of the $n$-gon allows to write any $g \in D_n$ as an orthogonal transformation (in fact a rotation or a symmetry). So we have a faithful representation

$$D_n \to \mathrm{O}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R}).$$

Analogously, we can consider symmetries of polytopes in $\mathbb{R}^3$. For example, it is known that the group of rotations of an icosahedron is isomorphic to $A_5$, which gives a faithful representation

$$A_5 \to \mathrm{O}_3(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{R}).$$

EXAMPLE 11.1.4 (Finite groups of Lie type). The group $\mathrm{GL}_2(\mathbb{F}_q)$ by definition has a 2-dimensional representation over $\mathbb{F}_q$. Representations in characteristic $p$, especially over finite fields, are known as *modular* representation. Of course $\mathrm{GL}_2(\mathbb{F}_q)$ also has representations in characteristic $0$. For example, it is easy to see that $\mathrm{GL}_2(\mathbb{F}_q)$ has $6$ elements and permutes three non-zero vectors of $(\mathbb{F}_2)^2$. Therefore, it is isomorphic to $S_3$ and has a 3-dimensional representation in $k^3$ by permuting basis vectors described above.

EXAMPLE 11.1.5. Let $F/K$ be a finite Galois extension with Galois group $G$. Then $G$ acts on $F$ and this action is $K$-linear:

$$g(kf) = g(k)g(f) = kg(f)$$

. So if we consider $F$ as an $n$-dimensional vector space over $K$ (where remember that $n = |G|$), we get a faithful representation

$$G \to \mathrm{GL}_n(K).$$

EXAMPLE 11.1.6. Let $G$ be any finite group. Perhaps its most important representation is the regular representation defined as follows. Let $k[G]$ be a vector space with a basis indexed by elements of $G$. In other words, we have

$$k[G] = \left\{ \sum_{g \in G} a_g g \,|\, a_g \in k \right\}$$

We extend the action of $G$ on itself by left multiplication to a representation of $G$ on $k[G]$:

$$g_0 \left( \sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g (g_0 g)$$

In fact, the two last examples are related:

THEOREM 11.1.7 (Normal Basis Theorem). *Let $F/K$ be a finite Galois extension with a Galois group $G$. Then the action of $G$ on $F$ is isomorphic to the regular representation of $G$.*

This is called a normal basis because it implies (and means) that $F$ has a basis over $K$ which is indexed by elements of the Galois group, and such that the Galois group permutes them accordingly.

§11.2. **Category of Representations.** We can define the category $\mathrm{Rep}_k(G)$ of representations of $G$ as follows. Its objects are representations of $G$. Its morphisms are linear maps

$$L : V_1 \to V_2$$

which commute with the action of the group:

$$L(gv) = gL(v)$$

for any $g \in G$, $v \in V_1$. This linear maps are also known as *equivariant* maps. The goal is to describe this category as explicitly as possible, i.e. to classify all representations and all morphisms.

In the first approximation, this is accomplished by Maschke's theorem and Schur's Lemma, respectively. They are discussed below. But first we need a definition:

DEFINITION 11.2.1. A representation of $G$ in $V$ is called *irreducible* if $V$ has no proper $G$-invariant subspaces, i.e. sub-representations.

DEFINITION 11.2.2. A direct sum of representations $G : V_1$ and $G : V_2$ is a direct sum of vector spaces $V_1 \oplus V_2$ equipped with a component-wise action of $G$: $g(v_1, v_2) = (gv_1, gv_2)$. In other words, the matrix of $g$ is block-diagonal, with blocks that correspond to $V_1$ and $V_2$.

A basic question is whether any representation is isomorphic to a direct sum of irreducibles. Here are two standard examples.

EXAMPLE 11.2.3. The standard representation of $S_n$ in $k^n$ has two sub-representations:

$$V_1 = k(e_1 + \ldots + e_n) \quad \text{and} \quad V_2 = \{\sum a_i e_i \mid \sum a_i = 0\}.$$

It is easy to see that $k^n = V_1 \oplus V_2$ and that both of them are irreducible.

EXAMPLE 11.2.4. Consider a subgroup

$$G = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \subset \mathrm{GL}_2(\mathbb{F}_q)$$

and its representation in $(\mathbb{F}_q)^2$. Then $G$ has only one proper sub-representation, namely a subspace spanned by $e_1$. So $(\mathbb{F}_q)^2$ does not split as a direct sum of irreducibles.

Now the result:

THEOREM 11.2.5 (Maschke). *Suppose* $\mathrm{char}\, k$ *does not divide* $|G|$*. Then any representation* $V$ *of* $G$ *is a direct sum of its irreducible sub-representations.*

*Proof.* Arguing by induction on $\dim V$, it suffices to prove the following: if $U \subset V$ is a $G$-invariant subspace then there exists a $G$-invariant subspace $U'$ such that $V = U \oplus U'$. We will give two possible arguments.

For the first one, let's choose a complementary *vector subspace* $W$ and let $\pi : V \to V$ be a projector on $U$ along $W$, i.e. $\mathrm{Ker}\, \pi = W$ and $\pi|_U = \mathrm{Id}\,|_U$. We are going to average $\pi$, namely consider the linear operator $\pi_0 : V \to V$ defined as follows:

$$\pi_0(v) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}v)$$

(here we use that $|G|$ is coprime to characteristic). The main calculation is

$$\pi_0(hv) = \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}hv) = \frac{1}{|G|}\sum_{g\in G} h(h^{-1}g)\pi((h^{-1}g)^{-1}v) =$$

$$h\frac{1}{|G|}\sum_{g\in G}(h^{-1}g)\pi((h^{-1}g)^{-1}v) = h\frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}v) = h\pi_0,$$

i.e. $\pi_0$ is equivariant. It follows that

$$U' = \operatorname{Ker}\pi_0$$

is $G$-invariant. Since it is easy to check that

$$\pi_0|_U = \operatorname{Id}|_U,$$

this gives $V = U \oplus U'$, a direct sum of $G$-invariant subspaces.

The second argument only works if $k = \mathbb{R}$ or $\mathbb{C}$. In this case let $(\cdot,\cdot)$ be an inner product on $V$ and let's define another one by formula

$$(v, v')_0 = \frac{1}{|G|}\sum_{g\in G}(gv, gv').$$

Any positive linear combination of inner products is an inner product, and it is easy to check that $(\cdot,\cdot)_0$ is $G$-invariant (i.e. $(gv, gv')_0 = (v, v')_0$). If $U \subset V$ is a $G$-invariant subspace, we can just take $U'$ to be an orthogonal complement of $U$: equivariance of $(v, v')_0$ then implies that $U'$ is $G$-invariant. □

REMARK 11.2.6. The Maschke's theorem is sometimes expressed by saying that $\operatorname{Rep}_k(G)$ is a "semi-simple category". This means that each object is "semi-simple", i.e. isomorphic to a direct sum of simple objects (where simple=irreducible). One also says that any representation of a finite group (with $\operatorname{char} k$ coprime to $|G|$) is "completely reducible", i.e. isomorphic to a direct sum of irreducibles.

Next we understand morphisms in $\operatorname{Rep}_k(G)$. To simplify things, let's fix an irreducible representation $V$ and consider the algebra of all morphisms from $V$ to itself:

$$\operatorname{End}_G(V) = \{L \in \operatorname{Hom}_k(V, V) \mid L(gv) = gL(v)\}$$

(the multiplication in $\operatorname{End}_G(V)$ is just the composition of endomorphisms). So $\operatorname{End}_G(V)$ is a subalgebra of the matrix algebra $\operatorname{Hom}_k(V, V)$.

LEMMA 11.2.7 (Schur). $\operatorname{End}_G(V)$ *is a division algebra, i.e. any non-zero element of it is invertible. If* $k = \bar{k}$ *then* $\operatorname{End}_G(V) = k$ *is a subalgebra of scalar operators in* $\operatorname{Hom}_k(V, V)$.

*Proof.* Let $L \in \operatorname{End}_G(V)$. Then it is easy to check that $\operatorname{Ker} L$ and $\operatorname{Im} L$ are $G$-invariant subspaces of $V$. Since $V$ is irreducible, we conclude that either $L = 0$ or $L$ is invertible. So $\operatorname{End}_G(V)$ is a division algebra.

Now suppose that $k = \bar{k}$. We can give two proofs. For the first one, let $\lambda$ be an eigenvalue of $L$ and let

$$V_\lambda = \{v \in V \mid Lv = \lambda v\}$$

be the corresponding eigenspace. We claim that $V_\lambda$ is $G$-invariant: indeed if $v \in V_\lambda$ then

$$L(gv) = gL(v) = g(\lambda v) = \lambda(gv),$$

and so $gv \in V_\lambda$. Since $V$ is irreducible and $V_\lambda \neq 0$, it follows that $V_\lambda = V$, i.e. $L$ acts on $V$ by multiplication by $\lambda$.

For the second proof, notice that $\mathrm{End}_G(V)$ obviously contains $k$ as a subalgebra of scalar operators. Moreover, these scalar operators commute with anything in $\mathrm{End}_G(V)$, i.e. $k$ belongs to the center of $\mathrm{End}_G(V)$. So we can try to argue that in fact if $k = \bar{k}$ then $k$ is the only division algebra finite-dimensional over $k$ and such that $k$ is contained in its center. Indeed, let $D$ be such an algebra and let $\alpha \in D$. Let $k(\alpha)$ be the minimal division subalgebra containing $k$ and $\alpha$. Since $k$ and $\alpha$ commute, $k(\alpha)$ is in fact a field. This field is finite-dimensional over $k$, hence algebraic over $k$, but $k$ is algebraically closed, and so in fact $\alpha \in k$. □

We see that if $k$ is not algebraically closed then irreducible representations can be classified by a type of a division algebra that appears as its algebra of endomorphisms. For example, suppose $k = \mathbb{R}$. By a Theorem of Frobenius, finite-dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and quaternions $\mathbb{H}$. All these cases occur.

EXAMPLE 11.2.8. Let $C_n$ be a cyclic group with $n$ elements and consider its representation in $\mathbb{R}^2$ as the group of rotations of a regular $n$-gon. No lines in $\mathbb{R}^2$ are invariant under this action, so this representation is irreducible. It is easy to check that the algebra of endomorphisms in this case is $\mathbb{C}$. In fact, identifying $\mathbb{R}^2$ with $\mathbb{C}$ in the standard way, $C_n$ acts by multiplication by $n$-th roots on unity, and $\mathbb{C}$ acts simply by left multiplication. These two actions obviously commute.

EXAMPLE 11.2.9. Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of $8$ quaternions. It acts on all quaternions $\mathbb{H}$ by left multiplication. This gives an irreducible $4$-dimensional real representation ($\mathbb{H} \simeq \mathbb{R}^4$). Its equivariant endomorphisms are equal to $\mathbb{H}$ with the action on itself by *right* multiplication (notice that left multiplications by $Q_8$ and $H$ do not commute!).

§11.3. **Irreducible Representations of Abelian Groups.** Our next goal is to gather more specific information about irreducible representations. For example, we can ask how many of them are there, what are their dimensions, etc. This is going to depend on the field. To simplify matters, we are going to assume that $k$ is algebraically closed.

We start with Abelian groups.

LEMMA 11.3.1. *Let $G$ be an Abelian group. Then any irreducible representation of $G$ is $1$-dimensional and is given by some homomorphism $G \to \mathrm{GL}(k) = k^*$.*

*Proof.* Let $\rho : G \to \mathrm{GL}(V)$ be an irrep. For any $g_0 \in G$, $\rho(g_0)$ belongs to $\mathrm{End}_G(V)$. Indeed,

$$\rho(g_0)(gv) = \rho(g_0 g)(v) = \rho(g g_0)(v) = g\rho(g_0)v.$$

By Schur's Lemma, $\rho(g_0)$ must be a scalar linear operator. So $G$ acts by scalar operators, and therefore any vector subspace is $G$-invariant. It follows that $\dim V = 1$. □

To classify all irreducible representations, we introduce the following definition.

DEFINITION 11.3.2. Let $G$ be a finite Abelian group. Its *Pontryagin dual* group $\hat{G}$ is the group of all homomorphisms $\phi : G \to k^*$ with the multiplication given by

$$(\phi\psi)(g) = \phi(g)\psi(g).$$

The unit element in this group is the trivial homomorphism $G \to \{1\} \in k^*$.

So irreducible representations of $G$ are classified by elements of $\hat{G}$.

LEMMA 11.3.3. *Let $G$ be a finite Abelian group. Suppose $\operatorname{char} k$ is coprime to $|G|$. Then $\hat{G}$ is non-canonically isomorphic to $G$, in particular $|G| = |\hat{G}|$ and so $G$ has $|G|$ irreducible 1-dimensional representations. The map*

$$g \to [\phi \mapsto \phi(g)]$$

*is a canonical isomorphism between $G$ and $\hat{\hat{G}}$.*

*Proof.* Notice that $\widehat{G_1 \times G_2} \simeq \hat{G}_1 \times \hat{G}_2$ Indeed, a homomorphism $G_1 \times G_2 \to k^*$ is uniquely determined by its restrictions on $G_1$, $G_2$. And given homomorphisms $\phi_1 : G_1 \to k^*$, $\phi_2 : G_2 \to k^*$, we can define a homomorphism $\phi : G_1 \times G_2 \to k^*$ by formula $\phi(g_1, g_2) = \phi_1(g_1)\phi_2(g_2)$.

By the fundamental theorem on Abelian groups, we therefore can assume that $G \simeq \mathbb{Z}/n\mathbb{Z}$ is cyclic. A homomorphism $\mathbb{Z}/n\mathbb{Z} \to k^*$ sends $1$ to an $n$-th root of unity. So we see that $\widehat{\mathbb{Z}/n\mathbb{Z}} = \mu_n$. But $\operatorname{char} k$ is coprime to $|G|$, ad therefore coprime to $n$. So $|\mu_n| = n$ and $\mu_n$, as any finite subgroup of $k^*$, is cyclic. This shows the first statement.

Finally, we claim that $G$ is canonically isomorphic to its double dual. Since they have the same number of elements, it suffices to show that the map $g \to [\phi \mapsto \phi(g)]$ is injective. If it is not, then any homomorphism $\phi : G \to k^*$ vanishes on some $g \in G$. But then $\hat{G}$ can be identified with $\widehat{G/\langle g \rangle}$, and in particular $|\hat{G}| < |G|$, which is a contradiction. □

EXAMPLE 11.3.4. Let's classify all complex representations of $\mathbb{Z}/7\mathbb{Z}$. We have

$$\widehat{\mathbb{Z}/7\mathbb{Z}} = \mu_7,$$

the group of 7-th roots of unity in $\mathbb{C}^*$. For each root $\eta = e^{\frac{2pi}{7}k}$, the corresponding representation is

$$\mathbb{Z}/7\mathbb{Z} \to \mathbb{C}^*, \quad i \mapsto \eta^i.$$

It is also very easy to classify all 1-dimensional representations of an arbitrary group $G$.

DEFINITION 11.3.5. For any $g, h \in G$, the element $ghg^{-1}h^{-1}$ is called their commutator. Let $[G, G]$ be the subgroup of $G$ generated by all commutators. It is called a *commutant* of $G$.

LEMMA 11.3.6. *The commutant $[G, G]$ is a normal subgroup of $G$ and $G/[G, G]$ is Abelian. Moreover, if $H$ is normal in $G$ and $G/H$ is Abelian then $H \supset [G, G]$. There is a natural bijection between 1-dimensional representations of $G$,*

*i.e. homomorphisms $G \to k^*$, and 1-dimensional representations of $G/[G,G]$, i.e. $\widehat{G/[G,G]}$.*

*Proof.* The basic calculation is

$$a(ghg^{-1}h^{-1})a^{-1} = (aga^{-1})(aha^{-1})(aga^{-1})^{-1}(aha^{-1})^{-1},$$

i.e. the set of all commutators is preserved by inner automorphisms. It follows that $[G,G]$ is preserved by inner automorphisms, i.e. $[G,G]$ is a normal subgroup. For any cosets $g[G,G]$, $h[G,G]$, their commutator is

$$ghg^{-1}h^{-1}[G,G] = [G,G],$$

i.e. $G/[G,G]$ s Abelian.

If $f : G \to G'$ is a homomorphism then $[G,G]$ is obviously mapped into $[G',G']$. It follows that if $G'$ is Abelian then $[G,G]$ is contained in $\operatorname{Ker} f$. In particular, there is a bijection between homomorphisms $G \to k^*$ and $(G/[G,G]) \to k^*$. □

For example, let's take $S_n$. It is not hard to check that $[S_n, S_n] = A_n$, and therefore $S_n$ has 2 1-dimensional representations. One is a trivial representation,

$$S_n \to k^*, \quad g \mapsto 1.$$

Another is the sign representation,

$$S_n \to k^*, \quad g \mapsto \operatorname{sgn}(g).$$

§11.4. **Characters.**

From now on we are going to work over $\mathbb{C}$. The reason for this is that we are going to use Hermitian inner products, which are not available over arbitrary fields. However, all results that we prove can be proved over arbitrary algebraically closed fields of characteristic not dividing $|G|$ by using slightly more abstract methods.

DEFINITION 11.4.1. Let $\rho : G \to \mathrm{GL}(V)$ be a representation of $G$. Its character $\chi$ is a function $G \to \mathbb{C}$ defined as follows:

$$\chi(x) = \operatorname{Tr} \rho(x)$$

for any $x \in G$.

Recall that $\mathbb{C}[G]$ denotes the space of formal linear combinations $\sum_{g\in G} a_g[g]$, which we frequently interpret as functions $G \to \mathbb{C}$, $g \mapsto a_g$. So we can think about each character as an element of $\mathbb{C}[G]$. In fact, we can say more.

DEFINITION 11.4.2. An function $G \to \mathbb{C}$ is called a *class function* if it is constant on conjugacy classes.

LEMMA 11.4.3. *Each character is a class function.*

*Proof.* Indeed,

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

So $\chi$ is constant on conjugacy classes. □

EXAMPLE 11.4.4. Consider the standard action of $S_n$ on $\mathbb{C}^n$ by permuting basis vectors. For any $\sigma \in S_n$, we have $\chi(\sigma) = \operatorname{Tr}(\sigma)$ is equal to the number of elements of $\{1, \dots, n\}$ fixed by $\sigma$.

EXAMPLE 11.4.5. Notice that

$$\chi(e) = \mathrm{Tr}(\mathrm{Id}) = \dim V$$

for any representation of $G$.

EXAMPLE 11.4.6. Consider the regular representation. Recall that $G$ acts on $\mathbb{C}[G]$ by formula

$$h(\sum_{g\in G} a_g[g]) = \sum_{g\in G} a_g[hg].$$

Notice that if $h \neq e$ then the matrix of $h$ has no diagonal entries at all (as $g \neq hg$ for any $g \in G$), and so we have

$$\chi_{reg}(x) = \begin{cases} |G| & \text{if } x = e \\ 0 & \text{if } x \neq e \end{cases}$$

It turns out that characters behave very naturally with respect to various basic operations with representations:

THEOREM 11.4.7. *We have*

$$\chi_{V\oplus W} = \chi_V + \chi_W,$$
$$\chi_{V\otimes W} = \chi_V \chi_W,$$
$$\chi_{V^*} = \overline{\chi_V},$$
$$\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V}\chi_W.$$

*Proof.* We are going to be lazy and use the fact that the trace is the sum of eigenvalues and that $\rho(g)$ is diagonalizable for any $g \in G$ and any representation $\rho$ (as a linear operator of finite order).

$G$ acts on $V \oplus W$ by formula $g(v, w) = (gv, gw)$. The matrix of this representation is a block-diagonal matrix of representations in $V$ and $W$, and the trace is obviously additive.

$G$ acts on $V \otimes W$ by formula $g(v \otimes w) = gv \otimes gw$. This is well-defined: a bilinear map $G : V \times W \to V \otimes W$ defined as $G(v, w) = (gv) \otimes (gw)$ induces a linear map $v \otimes w \mapsto (gv) \otimes (gw)$. Notice that if $v_1, \ldots, v_n$ (resp. $w_1, \ldots, w_m$) are eigenvectors for $\rho(g)$ in $V$ (resp. in $W$) with eigenvalues $\lambda_1, \ldots, \lambda_n$ (resp. $\mu_1, \ldots, \mu_m$) then $\{v_i \otimes w_j\}$ are eigenvectors for $\rho(g)$ in $V \otimes W$ with eigenvalues $\lambda_i\mu_j$. We have

$$\chi_{V\otimes W}(g) = \sum_{i,j} \lambda_i\mu_j = (\sum_i \lambda_i)(\sum_j \mu_j) = \chi_V(g)\chi_W(g).$$

$G$ acts on $V^*$ as follows: if $f \in V^*$ is a linear map $v \mapsto f(v) \in \mathbb{C}$ then $\rho_{V^*}(g)f$ is a linear map

$$v \mapsto f(\rho(g^{-1})v).$$

This looks funny, but in fact this is the only way to ensure that $\rho_{V^*}$ is a homomorphism, i.e. that $\rho_{V^*}(gh) = \rho_{V^*}(g)\rho_{V^*}(h)$. This is the standard formula: each time the group $G$ acts on a space $X$, it acts linearly on the space of functions on $X$ by a formula above. The matrix of $\rho_{V^*}(g)$ can be obtained from the matrix of $\rho_V(g)$ by transposing and inverting

□

## §11.5. **Schur Orthogonality Relations.**

§11.6. **Decomposition of the Regular Representation.**

§11.7. **Representation Theory of the Dihedral Group.**

§11.8. **The Number of Irreducible Representations.**

§11.9. $\mathbb{C}[G]$ **as an Associative Algebra.** We have already used the fact that any $f \in \mathbb{C}[G]$ acts in any representation $V$ of $G$ "linearly extending" the action of $G$. This fact can be refined as follows.

DEFINITION 11.9.1. We define a binary operation on $\mathbb{C}[G]$ by formula

$$[g] \star [h] = [gh]$$

extended by linearity. This makes $\mathbb{C}[G]$ into an associative algebra, called the *group algebra*. (the product is associative because the multiplication in $G$ is associative). This algebra has a unit, namely $[e] \in \mathbb{C}[G]$.

If we think about elements of $\mathbb{C}[G]$ as functions $G \to \mathbb{C}$, the product is known as *the convolution product*: for any functions $\alpha, \beta : G \to \mathbb{C}$, we have

$$\alpha \star \beta(g) = \sum_{h \in G} \alpha(h)\beta(h^{-1}g).$$

The following basic fact enhances the observation we already made that the size of the group is equal to the sum of squares of dimensions of irreducible representations. In it we use the following common notation: if $V$ is a $k$-vector space then we denote by $\mathrm{End}(V)$ the algebra of all $k$-linear operators $V \to V$ (sometimes called *endomorphisms*) with an operation given by composition of linear operators. Of course this is just a coordinate-free version of the matrix algebra $\mathrm{Mat}_n(k)$ (where $n = \dim V$).

LEMMA 11.9.2. $\mathbb{C}[G]$ *with the convolution product is isomorphic to the direct sum*

$$\mathrm{End}(V_1) \times \ldots \times \mathrm{End}(V_r)$$

*over all irreducible representations.*

*Proof.* For each $f \in \mathbb{C}[G]$, $\rho_i(f)$ is an endomorphism of $V_i$. It is easy to see that this gives a homomorphism

$$\mathbb{C}[G] \to \mathrm{End}(V_1) \times \ldots \times \mathrm{End}(V_r).$$

We already know that both sides have the same dimension. So it suffices to show that the map is injective. But if $f = \sum a_g[g] \in \mathbb{C}[G]$ acts trivially on each irreducible representation, it acts trivially on any representation whatsoever, including the regular representation. But we have

$$f \star [e] = f$$

is not trivial. □

As a digression, let's discuss how one can develop the representation theory of finite groups over an arbitrary field $k$ of characteristic not dividing $|G|$. The Schur orthogonality is not going to work because hermitian inner products are specific to $\mathbb{C}$. Instead, the Lemma above will play the foundational role: one can prove it directly using the general theory of associative algebras.

More precisely, let's consider the group algebra $k[G]$ (here $k$ is any field of characteristic not dividing $|G|$). This is an example of an associative algebra with a unit. Another example of such an algebra is $\mathrm{End}(V)$. We can talk about a representation of an associative algebra $R$ in a vector space $V$: it is given by a homomorphism $R \to \mathrm{End}(V)$. We can define irreducible representations, etc. Notice that the category of representations of $k[G]$ is equivalent to the category of representations of $G$ (by extending any homomorphism $G \to \mathrm{GL}(V)$ to a homomorphism $k[G] \to \mathrm{End}(V)$ by linearity). So the Maschke's theorem implies that the category of representations of $k[G]$ is semi-simple: any representation is isomorphic to a direct sum of irreducible representations. So $k[G]$ is an example of a semi-simple algebra:

DEFINITION 11.9.3. A finite-dimensional associative algebra $R$ (with a unit) is called *semi-simple* if any finite-dimensional representation of $R$ is isomorphic to a direct sum of irreducible representations.

One has the following amazing structure theorem:

THEOREM 11.9.4 (Wedderburn–Artin). *Suppose $k$ is algebraically closed. Then $R$ has finitely many irreducible representations $V_1, \dots, V_r$ and*

$$R \simeq \mathrm{End}(V_1) \times \ldots \times \mathrm{End}(V_r).$$

We see that Lemma 11.9.2 is a formal corollary of this very general result (the proof of this theorem is not at all difficult, see any textbook).

In fact, one can remove the assumption that $k = \bar{k}$. In this case the Schur's lemma implies that $\mathrm{End}_R(V_i)$ (endomorphisms that commute with the action of $R$) is a division algebra $D_i$ for each irreducible representation $V_i$, and then one has

$$R \simeq \mathrm{End}_{D_1}(V_1) \times \ldots \times \mathrm{End}_{D_r}(V_r),$$

the direct sum of matrix algebras over division algebras $D_1, \dots, D_r$.

So, for example, if $G$ is a finite group then $\mathbb{R}[G]$ is a direct sum of matrix algebras over $\mathbb{R}$, $\mathbb{C}$, and the quaternions $\mathbb{H}$.

## §11.10. $\dim V_i$ **divides** $|G|$**.**

THEOREM 11.10.1. *Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation of a finite group $G$. Then $\dim V$ divides $|G|$.*

*Proof.* Recall that the integral closure $\bar{\mathbb{Z}}$ of $\mathbb{Z}$ in $\mathbb{C}$ is called *the ring of algebraic integers*. These numbers are roots of monic polynomials with integer coefficients. For example, $\chi_V(g) \in \bar{\mathbb{Z}}$ for any $g \in G$. Indeed, $\rho(g)$ is a matrix such that $\rho(g)^k = \mathrm{Id}$ for $k = \mathrm{ord}(g)$, and therefore all eigenvalues of $\rho(g)$ are $k$-th roots of unity. But any rot of unity is an algebraic integer. So $\chi_V(g)$ is also an algebraic integer as the sum of these eigenvalues.

Let $C \subset G$ be a conjugacy class and let

$$I_C = \sum_{g \in C} [g]$$

be its characteristic function. It follows from the definition that $I_C \star I_{C'}$ is an integral linear combination of group elements, and therefore we can write

$$I_C \star I_{C'} = \sum n_{C''} I_{C''}$$

for some integers $n_{C''}$. Next we look how both sides act on $V$. Since $I_C$ is a class function, it acts by scalar $\lambda_C$ and we have

$$\lambda_C \lambda_{C'} = \sum n_{C''} \lambda_{C''}.$$

Let $C_1, \dots, C_r$ be all conjugacy classes of $G$. Then we have

$$\lambda_C \begin{bmatrix} \lambda_{C_1} \\ \vdots \\ \lambda_{C_r} \end{bmatrix} = A \begin{bmatrix} \lambda_{C_1} \\ \vdots \\ \lambda_{C_r} \end{bmatrix}$$

for some integral matrix $A$. This column-vector is non-trivial, for example $\lambda_{\{e\}} = 1$. It follows that each $\lambda_C$ is an eigenvalue of an integral matrix, and therefore each $\lambda_C$ is an algebraic integer.

Now we use Schur's orthogonality:

$$1 = (\chi_V, \chi_V) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_V(g)} =$$

$$\frac{1}{|G|} \sum_{i=1}^{r} |C_i| \chi_V(g_i) \overline{\chi_V(g_i)} = \frac{1}{|G|} \sum_{i=1}^{r} \mathrm{Tr}_V(I_{C_i}) \overline{\chi_V(g_i)} \frac{1}{|G|} \sum_{i=1}^{r} \dim V \lambda_{C_i} \overline{\chi_V(g_i)}$$

for some $g_i \in C_i$. It follows that

$$\frac{|G|}{\dim V} = \sum_{i=1}^{r} \lambda_{C_i} \overline{\chi_V(g_i)}$$

is an algebraic integer. But it is also a rational number, and so must be an integer since $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ (if a rational number $r$ is a root of a monic polynomial with integer coefficients, $r$ must be an integer). □

§11.11. **Burnside's Theorem.** As an application of developed techniques, let's prove the following theorem of Burnside:

THEOREM 11.11.1. *Any group of order $p^a q^b$, where $p$ and $q$ are primes, is solvable.*

This is of course a vast improvement over similar but much simpler results obtained last semester using naive techniques. When Burnside proved this result, he made an astonishing conjecture that in fact any finite group of odd order is solvable. This was proved in 1963 by Feit and Thompson in a dense 250-page long argument, which many at the time thought was the most complicated proof ever. The theorem of Feit and Thompson is often considered to be the start of the classification of finite simple groups, which was completed after Fischer and Griess discovered their Monster, the largest sporadic simple group of order $8 \cdot 10^{53}$.

The proof of Burnside's theorem is based on the following lemma:

LEMMA 11.11.2. *Suppose a finite group $G$ has a conjugacy class $C$ of size $p^k$, where $p$ is prime and $k > 0$. Then $G$ has a proper normal subgroup.*

Given the lemma, let's see how to finish the proof the proof of Burnside's theorem. Arguing by induction, it suffices to prove that $G$ has a proper normal subgroup. Since a $p$-group has a non-trivial center, we can assume that $p \neq q$ and $a, b > 0$. Let $H$ be a Sylow $q$-group. Let $x$ be a non-trivial element of the center of $H$. Let $Z(x)$ be the the centralizer of $x$ in $G$. If

$Z(x) = G$ then the cyclic group generated by $x$ is a proper normal subgroup of $G$. If $Z(x) \neq G$ then $[G : Z(x)] = p^k$ for some $k > 0$ (because $H \subset Z(x)$). But $[G : Z(x)]$ is equal to the number of elements in the conjugacy class of $x$, and therefore $G$ contains a proper normal subgroup by the Lemma.

It remains to prove the lemma.

*Proof of the Lemma.* Recall that we have a decomposition of the regular representation

$$\mathbb{C}[G] = V_{reg} \simeq \bigoplus_{i=1}^{r} d_i V_i,$$

where each irreducible representation appears $d_i = \dim V_i$ times. Also recall that

$$\chi_{reg}(x) = \begin{cases} |G| & \text{if } x = e \\ 0 & \text{if } x \neq e \end{cases}$$

Let $x \in C$. By additivity of characters, we have

$$0 = 1 + \sum_{\chi \neq 1} d_\chi(x)\chi(x),$$

the summation over all non-trivial irreducible characters. Let's concentrate on irreducible representations such that $p \not| d_\chi$.

Notice that $\chi(x) \neq 0$ for one of such irreps: otherwise we would be able to write $1/p$ as an integral linear combination of characters, which would imply that $1/p$ is an algebraic integer, which is impossible because $1/p$ is a rational number but not an integer.

Also notice that if $x$ acts in $V_\chi$ by a scalar matrix then $G$ has a proper normal subgroup, namely the preimage of the normal subgroup $\mathbb{C}^* \operatorname{Id} \subset \operatorname{GL}(V_\chi)$ (this preimage is not equal to $G$ because $V_\chi$ is irreducible).

The claim, however, is that one of these two things must happen.

CLAIM 11.11.3. *Let $\rho : G \to \operatorname{GL}(V)$ be an irreducible representation with character $\chi$ and let $C$ be a conjugacy class in $G$ such that $|C|$ and $\dim V$ are coprime. If $x \in C$ then either $\chi(x) = 0$ or $\rho(x)$ is a scalar linear operator.*

Indeed, choose $p$ and $q$ such that

$$p|C| + q \dim V = 1.$$

Then

$$p\frac{\chi(x)|C|}{\dim V} + q\chi(x) = \frac{\chi(x)}{\dim V}.$$

In the proof of "divisibility" Theorem 11.10.1, we have noticed that

$$\frac{\chi(x)|C|}{\dim V} = \lambda_C$$

is an algebraic integer. So we see that, in our case, $\alpha := \frac{\chi(x)}{\dim V}$ is also an algebraic integer. Notice that $\chi(x) = \zeta_1 + \ldots + \zeta_d$ is a sum of $d = \dim V$ $n$-th roots of unity (where $n$ is the order of $x$ in $G$).

There are two possibilities: either all these eigenvalues $\zeta_i$ are equal (in which case $\rho(x)$ is a scalar operator) or they are not equal, in which case

$$|\alpha| = \frac{1}{d}|\zeta_1 + \ldots + \zeta_d| < 1.$$

However, we claim that this is impossible. Let $L$ be the cyclotomic field spanned by $n$-th roots of unity. Any element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ preserves the set of $n$-th roots of unity, and therefore

$$|\sigma(\alpha)| = \frac{1}{d}|\sigma(\zeta_1) + \ldots + \sigma(\zeta_d)| < 1.$$

It follows that the norm of $\alpha$

$$\beta := N(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \sigma(\alpha) \in \mathbb{Q}$$

also satisfies $|\beta| < 1$. But each $\sigma(\alpha)$ is an algebraic integer, therefore $\beta$ is an algebraic integer, and so $\beta \in \mathbb{Z}$. This gives a contradiction. □

§11.12. **Exercises.**

In this worksheet the base field is always $\mathbb{C}$ unless otherwise stated.

**1.** Describe explicitly (i.e. not just dimensions but how each element of the group acts) all irreducible representations of (a) $(\mathbb{Z}/2\mathbb{Z})^r$; (b) $D_{2n}$.

**2.** Describe explicitly all irreducible representations and build a character table for (a) $S_3$; (b) $A_4$; (c) the quaternionic group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

**3.** (a) Let $V$ be the standard $(n-1)$-dimensional representation of $S_n$ and let $\mathrm{sgn}$ be the 1-dimensional sign representation. Find all $n$ such that $V \simeq V \otimes \mathrm{sgn}$. (b) Describe explicitly all irreducible representations of $S_4$.

**4.** Let $G$ be the group of affine transformations of $\mathbb{F}_7$ of the form $x \mapsto ax + b$, where $a, b \in \mathbb{F}_7$ and $a^3 = 1$. (a) Show that $|G| = 21$ and describe its conjugacy classes. (b) Describe explicitly all irreducible complex representations of $G$. (c) Let $V$ be the 7-dimensional representation of $G$ in the algebra of functions $\mathbb{F}_7 \to \mathbb{C}$ induced by the action of $G$ on $\mathbb{F}_7$ by affine transformation. Decompose $V$ as a direct sum of irreducible representations.

**5.** Let $V$ be an irreducible representation of a finite group $G$ over $\mathbb{R}$. (a) Show that the complexification $V \otimes_{\mathbb{R}} \mathbb{C}$ is naturally a representation of $G$ over $\mathbb{C}$. (b) This representation is either irreducible or a direct sum of two irreducible representations. (c) Show on examples that both possibilities in (b) do occur.

**6.** Let $M$ be a module over a commutative ring $R$. Let $M^{\otimes k} = M \otimes_R \ldots \otimes_R M$ ($k$ times). Let $\Lambda^k M$ be a quotient module of $M^{\otimes k}$ by a submodule generated by all elements of the form $x_1 \otimes \ldots \otimes x_k$ where $x_i = x_j$ for some $i$ and $j$. For any decomposable tensor $x_1 \otimes \ldots \otimes x_k \in M^{\otimes k}$, its image in $\Lambda^k M$ is denoted by $x_1 \wedge \ldots \wedge x_k$. Show that if $M$ is a free $R$-module of rank $n$ with basis $e_1, \ldots, e_n$ then $\Lambda^k M$ is a free $R$-module of rank $\binom{n}{k}$ with basis $e_{i_1} \wedge \ldots \wedge e_{i_k}$ for all $1 \le i_1 < \ldots < i_k \le n$.

**7.** (a) Show that if $V$ is a representation of $G$ (over a field) then $\Lambda^k V$ is also a $G$-representation. (b) Let $V_1$ and $V_2$ be $G$-representations. Show that

$$\Lambda^k(V_1 \oplus V_2) \simeq \sum_{a+b=k} \Lambda^a V_1 \otimes \Lambda^b V_2.$$

**8.** (a) Let $V$ be a representation of $G$ with character $\chi_V$. Show that

$$\chi_{\Lambda^2 V}(g) = \frac{1}{2}\left(\chi_V(g)^2 - \chi_V(g^2)\right).$$

(b) Let $V$ be the standard $4$-dimensional irreducible representation of $S_5$. Show that $\Lambda^2 V$ is an irreducible $6$-dimensional representation.

**9.** Let $V$ be an irreducible representation of a finite group $G$. Show that there exists a unique $G$-invariant hermitian inner product on $V$.

**10.** Show that the columns of the character matrix are orthogonal, and more precisely that

$$\sum_{\chi} \chi(g)\overline{\chi(g)} = \frac{|G|}{c(g)},$$

where the summation is over all irreducible characters of $G$ and $c(g)$ is the number of elements of $G$ conjugate to $g$. Also show that

$$\sum_{\chi} \chi(g)\overline{\chi(g')} = 0$$

if $g$ and $g'$ are not conjugate.

**11.** In this problem $k = \mathbb{F}_q$ is a finite field with $q = p^n$ elements. Let $G$ be a $p$-group. Show that the trivial representation is the only irreducible representation of $G$ over $k$.

**12.** For any two $2$-dimensional representations $V_1$ and $V_2$ of $D_{11}$, decompose $V_1 \otimes V_2$ as a direct sum of irreducible representations.

**13.** Let $V$ be a faithful representation of $G$ (i.e. the homomorphism $G \to \mathrm{GL}(V)$ is injective). Show that any irreducible representation of $G$ is contained in a tensor power $V^{\otimes n}$ for some $n$.