BASIC ALGEBRA COURSE

1. Rings, modules

1.1. **Basic definitions.** One of the basic notions in Algebra is that of a ring.

1.1.1. **Definition.** An associative ring (with unit) is an abelian group R (with respect to the operation denoted as $+$) with an extra operation called product or multiplication, satisfying the following properties.

1. Associativity $a(bc) = (ab)c$, for all $a, b, c \in R$.
2. Existence of unit 1, $1a = a1 = a$, for all $a \in R$.
3. Distributivity:

$$a(b + c) = ab + ac,\ (a + b)c = ac + bc,$$

for all $a, b, c \in R$.

Nice examples of rings include

0. Fields.
1. Commutative rings like the polynomial ring $\mathbb{F}[x]$.
2. Group ring. It is non-commutative if the group is not commutative. Given a group G and a field k (any commutative ring instead of k will work as well), we define the group ring kG as the vector space spanned by the elements $g \in G$. That is, kG as an additive group is the set of finite linear combinations $\sum a_i g_i$ where $a_i \in k$ and $g_i \in G$. The multiplication is uniquely determined by the multiplication in G and the distributivity law.
3. Matrix ring. The ring $M_n(k)$ of square matrices of size n over a field k (one could replace it with any ring, actually) has been studied in the Linear algebra course.
4. Weyl algebra. Will be defined in exercises.

One can think of a ring as a (far) generalization of a field. Modules are generalizations of vector spaces.

1.1.2. **Definition.** A (left) module over a ring R is an abelian group $(M, +)$ with an extra operation of (left) multiplication by elements of R. The axioms include:

- Two distributivity laws. That is,

$$(a + b)m = am + bm,\ a(m + n) = am + an$$

for $a, b \in R,\ m, n \in M$.

- Associativity of multiplication by scalar, $a(bm) = (ab)m$ for $a, b \in R$ and $m \in M$.
- Unit acts as identity, $1m = m$ for $m \in M$.

One could have defined right modules. This would lead to a parallel but not identical notion (as the multiplication in a ring needs not to be commutative).

1.1.3. **Definition.** Let R be a ring. The opposite ring R^{op}, is defined as follows. As the additive group, they are the same: $(R^{\mathrm{op}}, +) = (R, +)$. The multiplication in R^{op} (we deinte it by $*$ to distinguish from the original multiplication) is defined by the formula $a * b = ba$.

If R is commutative, $R = R^{\mathrm{op}}$. Sometimes R is isomorphic to R^{op}, but in a nontrivial way. For instance, a group ring is isomorphic to its opposite, find the isomorphism (Hint: the isomorphism $kG \to (kG)^{\mathrm{op}}$ carries $g \in G$ to g^{-1}).

Weyl algebra is also isomorphic to its opposite in a nontrivial way.

1.1.4. **Proposition.** *Left modules over R are "the same as" right modules over R^{op} (and vice versa).*

Modules are like vector spaces over general rings. However, they are not really like vector spaces.

1.1.5. **Definition.** (Module generated by a set) Let R be a ring, M an R-module, $X \subset M$ a subset. We will say that X generated M if any $m \in M$ can be presented as a (finite) linear combination

$$m = \sum a_i x_i, \quad a_i \in R,\ x_i \in X.$$

The definition above looks precisely as the definition of generating set in linear algebra. The main difference of the notion of module with the notion of a vector space is that modules usually do not have a basis, that is a generating set for which any element as a unique presentation as a linear combination.

1.1.6. **Definition.** Let M be a module over R. A left submodule of M is defined as an additive subgroup $N \subset M$ such that

$$a \in R,\ x \in N \Longrightarrow ax \in N.$$

The ring R is obviously a left module over itself. As a special case of a previous definition, we get a notion of left ideal.

1.1.7. **Definition.** A left ideal I in a ring R is an additive subgroup $I \subset (R, +)$ satisfying the property

$$x \in I,\ a \in R \Longrightarrow ax \in I.$$

Since R is a left module over R, a left ideal is just a left submodule of R.

Given a left R-module M and a submodule N of M, one defines M/N, the quotient module, as the additive factor group $M/N = \{m+N\}$ endowed with the left multiplication by the elements of R given by the formula $a(m+N) = am+N$.

A standard *Isomorphism theorem* claims that if $f : M \to N$ is a surjective homorphism of R-modules with the kernel K then N is naturally isomorphic to the quotient M/K.

1.1.8. We are now able to describe all R-modules generated by one element.

Let M be generated by $x \in M$. That is any element has form ax for some $a \in R$. This defines a surjective map $R \to M$ carrying a to ax. This is a linear map. Let us describe its kernel $I = \{a \in R | ax = 0\}$. Obviously, if $x \in I$ and $a \in R$ then $ax \in I$, that is, I is a left ideal. We will now describe the module M generated by $x \in M$ as the quotient R/I.

Note that the module $M = R/I$ does not have a basis. It is generated by one element $x := 1 + I$, so that any element of M has form $ax(= a + I)$. But this presentation is not unique, unless $I = 0$ (we write this instead of formally more correct $I = \{0\}$).

We can already note that modules over general rings are different from vector spaces.

- There are non-isomorphic modules generated by one element.
- Most of them have no basis.
- A surjective map $M \to N$ of modules does not necessarily split.
- An injective map of modules $N \to M$ does not necessarily split.

The last two claims require explanation. Let k be a field and let V, W be k-vector spaces. Let $f : V \to W$ be a linear map. If f is surjective, there exists $g : W \to V$ such that $f \circ g = \mathrm{id}_W$. One describes this saying that f is right-invertible (or that f splits). If f is injective, there exists $g : W \to V$ such that $g \circ f = \mathrm{id}_V$, that is, f is left invertible.

Usually the surjective map $R \to R/I$ does not split (as well as the injective map $I \to R$).

1.1.9. *Example.* $R = M_n(k)$, the matrix ring, $M = k^n$, the vector space of columns of length n. The left multiplication of elements of M by the elements of R is given by matrix multiplication.

1.1.10. *Exercise.* Prove that R is a direct sum of n modules isomorphic to M, see the above example.

1.1.11. *Exercises.*

1. Describe modules over $\mathbb{Z}$.
2. Give an example of an epimorphism of $\mathbb{Z}$-modules that does not split.

We have forgotten to define homomorphism of modules. Here it is.

1.1.12. **Definition.** A homomorphism of left R-modules $f : M \to N$ is a homomorphism of additive groups satisfying the extra condition

$$f(am) = af(m), \quad a \in R, m \in M.$$

1.1.13. **Definition.**

1. A sequence of R-modules and homomorphisms

$$\ldots \to M_{k+1} \stackrel{d_{k+1}}{\to} M_k \stackrel{d_k}{\to} M_{k-1} \stackrel{d_{k-1}}{\to} \ldots$$

is called *a complex* if $d_k \circ d_{k+1} = 0$. In other words, if $\mathrm{Ker}(d_k) \supset Im(d_{k+1})$ for all k.

2. A complex is *exact* at M_k if there is an equality $\mathrm{Ker}(d_k) = Im(d_{k+1})$. A complex is exact if it is exact at M_k for all k.

A short exact sequence is an exact sequence

$$0 \to M \to N \to K \to 0.$$

Please verify that

1. $0 \to M \stackrel{f}{\to} N$ is exact iff f is injective.
2. $M \stackrel{f}{\to} N \to 0$ is exact iff f is surjective.

1.2. **Split exact sequences.**

1.2.1. **Definition.** A monomorphism $f : M \to N$ is called split if there exists $s : N \to M$ such that $sf = \mathrm{id}_M$. An epimorphism $g : N \to K$ is called split if there exists $t : K \to N$ such that $gt = \mathrm{id}_K$.

1.2.2. **Lemma.** *Let $M \stackrel{f}{\to} N \stackrel{g}{\to} K$ be a short exact sequences. Then f is split iff g is split.*

Proof. Assume g is split, that is, $gt = \mathrm{id}_K$. We claim that $N = f(M) \oplus t(K)$. In fact, the intersection is trivial: if $f(x) = t(y)$ then $0 = gf(x) = gt(y) = y$ so $y = 0$ and $f(x) = 0$. Since f is injective, $x = 0$. On the other hand, for any $z \in N$ $z - tg(z)$ belongs to the kernel of g (verify!), so to the image of f. Thus, $z = f(x) + tg(z) \in t(K) + f(M)$.

We can now define the map $s : N \to M$ splitting f by the formula $s(f(x) + t(y)) = x$.

The converse is similar. □

A short exact sequence satisfying the above lemma is called split. As we saw from the proof, split short exact sequences are isomorphic to $M \to M \oplus K \to K$, with $f(x) = (x, 0)$ and $g(x, y) = y$.

1.3. **Simple modules.** A module is simple if it is nonzero and has no nontrivial submodules.

1.3.1. **Lemma.** *(Schur lemma) Let M, N be simple modules, $f : M \to N$ a module homomorphism. Then either $f = 0$ or f is an isomorphism.*

1.3.2. *Ring of endomorphisms of a module.* Given a ring R and an R-module M, the ring $\mathrm{End}_R(M)$ is defined as follows.

- As an abelian group, this is the group of R-momomorphisms from M to M with respect to addition.
- Multiplication is defined by composition.

In the special case R is a field and M is the vector space R^n, $\mathrm{End}_R(M)$ is the matrix ring $M_n(R)$.

According to the Schur's lemma, endomorphisms of a simple module form a division ring, that is a ring (not necessarily commutative) where all nonzero elements are invertible.

Example of a division ring that is not a field: the algebra of quaternions.

1.3.3. **Definition.** The algebra of quaternions Q is generated over $\mathbb{R}$ by for elements $1, i, j, k$. Multiplication is defined on the generators by the formulas

- 1 is the unit.
- $i^2 = j^2 = k^2 = -1$.
- $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

Exercise: One could have replaced in the above definition $\mathbb{R}$ with $\mathbb{C}$ and get a ring that is a 4-dimensional vector space over $\mathbb{C}$. Prove it is isomorphic to $M_2(\mathbb{C})$.

1.3.4. *Exercise.* Let R be a ring, describe the endomorphism ring of R as a left module over itself. Answer: This is R^{op}.

1.3.5. **Definition.** A ring R is called semisimple iff it is a direct sum of simple modules.

We will prove soon the following Wedderburn-Artin theorem.

Theorem. Let R be semisimple. Then R is a finite product of matrix rings over division algebras.

1.4. **Direct sum and direct product.**

1.4.1. We will describe the operations of direct sum and direct product of modules over a (fixed) ring A. These two operations give the same asnwer when the number of summands is finite; in general the sum is a submodule of the product.

So, let A be a ring and M_i, $i \in I$, is a collection of A-modules. Their direct product $M = \prod_{i \in I} M_i$ is defined as follows.

1. As a set, M is the cartesian product of M_i, that is, the set of collections $\{m_i,\ i \in I\}$, with $m_i \in M_i$.
2. The operations of sum and scalar multiplication are defined componentwise: $\{m_i\} + \{n_i\} = \{m_i + n_i\}$ and $a\{m_i\} = \{am_i\}$.

The direct sum of M_i, $N := \oplus_{i\in I} M_i$ (sometimes denoted as $\coprod_{i\in I} M_i$), is the submodule $N \subset \prod_{i\in I} M_i$ that consists of collections $\{m_i\}$ for which all but finite number of m_i are zero. In the case when I is a finite set both constructions yield the same result.

1.4.2. The following two elementary results may serve a good explanation for the difference between two constructions.

1.4.3. **Proposition.** *Let A be a ring, M and M_i, $i \in I$ are A-modules. A homomorphism $f : M \to \prod_{i\in I} M_i$ is uniquely given by a collection of homomorphisms $f_i : M \to M_i$. The assignment carries the collection of homomorphisms $f_i : M \to M_i$ to the homomorphism $f : M \to \prod M_i$ that carries $m \in M$ to the collection $f(m) = \{f_i(m)\}_{i\in I}$.*

□

1.4.4. **Proposition.** *Let A be a ring, M and M_i, $i \in I$ are A-modules. A homomorphism $f : \oplus_{i\in I} M_i \to M$ is uniquely given by a collection of homomorphisms $f_i : M_i \to M$. The assignment carries the collection of homomorphisms $f_i : M_i \to M$ to the homomorphism $f : \oplus M_i \to M$ that carries $\{m_i\} \in \oplus M_i$ to the element $f(\{m_i\}) = \sum_{i\in I} f_i(m_i)$. The latter formula makes sense as only a finite number of m_i is nonzero.*

□

The two propositions above mean that the notions of direct product and direct sum can be defined by *universal properties*. We wll discuss this later.

1.5. **Semisimplicity.** We will first study the notion of semisimple module.

1.5.1. **Theorem.** *The following conditions for a module M are equivalent.*

1. *M is a sum of its simple submodules.*
2. *M is a direct sum of (some of its) simple submodules.*
3. *Any embedding $N \to M$ splits.*

Proof. The implication $2 \Rightarrow 1$ is clear.

The implication $1 \Rightarrow 2$ requires Zorn lemma. We will find a maximal collection X of simple submodules S_x such that the sum $\sum S_x$ is direct, that is such that any element z in the sum has a unique presentation as $z = \sum y_x$ with $y_x \in S_x$ and the sum, of course, is finite.

This is done using Zorn lemma. We define a poset (=partially ordered set) of collections X satisfying the above property. It is nonempty (at least if $M \neq 0$) and it satisfies the requirement of Zorn lemma: any chain $X_1 \subset X_2 \subset \dots$ has an upper bound (just take the union). Let us prove that the sum $M' = \sum_{x\in X} S_x$ over the maximal collection X as described above gives the whole M. Assume $M \neq M'$. Since M is a sum of its simple submodules, there is a simple submodule

S of M such that S is not in M'. Then $S \cap M' = 0$ as S is simple. Then X is not maximal as one has a direct sum $S \oplus M'$.

Let us deduce $2 \Rightarrow 3$. Let $N \subset M$. Choose a maximal subset X of simple submodules such that the sum $N + \sum_{x \in X} S_x$ is a direct sum. Similarly to the above, we see that this sum is precisely M. This gives direct decomposition $M = N \oplus \sum_{x \in X} S_x$.

Finally, $3 \Rightarrow 1$. The most important is to prove that any nonzero submodule $N \subset M$ contains a simple submodule. Let $0 \neq x \in N$. Then N contains Rx (R is our ring), so we can assume $N = Rx$. We know that Rx is isomorphic to R/I where I is a left ideal of R. By Zorn lemma, there exists a maximal ideal J containing I. Hense Jx is a maximal submodule of Rx.

Let $M = Jx \oplus M'$. Then $Rx = Jx \oplus (M' \cap Rx)$. Since Jx is maximal in Rx, $M' \cap Rx$ is a simple module. □

Note that the equivalence of condition 3 to the rest of the condition is really nontrivial.

1.5.2. **Definition.** A module M is called semisimple if it satisfied the equivalent conditions of the above theorem.

1.5.3. **Lemma.** *Direct sum of semisimple modules is semisimple.*

Proof. Use property (2) of semisimple modules. □

1.5.4. **Lemma.** *Every submodule and factor module of a semisimple module is semisimple.*

Proof. Let $N \subset M$. In the proof of the theorem we saw that $M = N \oplus \sum_{x \in X} S_x$ for some collection X of simple modules. Then M/N is clearly a sum of simple modules. To prove N is a sum of simple modules, we can present it as a factor $M/\sum S_x$. □

1.5.5. **Definition.** A ring A is called semisimple if it is semisimple as a left module over itself.

1.5.6. **Theorem.** *(Wedderburn-Artin) Let A be a semisimple ring. Then it is a finite direct sum of simple modules. Let $A = L_1^{n_1} \oplus L_k^{n_k}$ be a decomposition of A into sum of simple modules, L_i and L_j being non-isomorphic for $i \neq j$. Then A is isomorphic to the direct product of rings $M_{n_i}(D_i)$.*

Proof. First of all, A is a direct sum of simple A-modules, $A = \oplus_{i \in I} L_i$. In particular, $1 = \sum x_i$ where $x_i \in L_i$. The last sum should be finite, and for any $a \in A$ we have $a = \sum a x_i$. Of course, $a x_i = 0$ if $x_i = 0$, so there is only finite number of summands.

Thus, $A = L_1^{n_1} \oplus \ldots \oplus L_k^{n_k}$ where L_i and L_j are not isomorphic when $i \neq j$. According to an exercise $\mathrm{End}_A(A) = A^{\mathrm{op}}$. This ring can now be canculated

differently. Since $\mathrm{Hom}_A(L_i, L_j) = 0$ for $i \neq j$,

$\mathrm{End}_A(A) = \mathrm{End}_A(L_1^{n_1} \oplus \ldots \oplus L_k^{n_k}) = \mathrm{End}(L_1^{n_1}) \times \ldots \times \mathrm{End}(L_k^{n_k}) = M_{n_1}(D_1) \times \ldots M_{n_k}(D_k)$.

It remains to mention that $M_n(D)^{\mathrm{op}}$ is isomorphic to $M_n(D^{\mathrm{op}})$. The isomorphism is given by transpose — we leave this as an exercise. □

1.5.7. **Corollary.** *If A is semisimple, then A^{op} is also semisimple.*

1.5.8. **Proposition.** *Let A be a semisimple ring. Then any A-module is semisimple.*

Proof. Let M be an A-module. We can choose a set X generating M (for instance, $X = M$). Let F be the free A-module spanned by X. Then one has a homomorphism of modules $f : F \to M$ carrying a generator $x \in X$ to the respective element of M. f is surjective. Now, F is a direct sum of X copies of A, therefore, semisimple. M is a factor-module of F, so is also semisimple. □

1.5.9. **Corollary.** *Any short exact sequence of modules over a semisimple algebra is split.*

1.6. **The category of modules.** We will start using some elementary notions connected to categories.

A category $\mathcal{C}$ is the following creature:

- It has a collection of objects (denoted $\mathrm{Ob}(\mathcal{C})$).
- For any two objects $x, y \in \mathrm{Ob}(C)$ we have a set $\mathrm{Hom}(x, y)$ called *the set of morphisms from x to y*. We often write $f : x \to y$ instead of $f \in \mathrm{Hom}(x, y)$. We whire $\mathrm{Hom}_{\mathcal{C}}(x, y)$ to indicate what category we are talking about.
- Given $f : x \to y$ and $g : y \to z$, a "composition" morphism $gf : x \to z$ is defined.
- The composition is associative and have "units" - morphisms $\mathrm{id}_x : x \to x$ that behave as unit with respect to the composition.

1.6.1. *Example: the category of sets.* We define the category `Set` as folows. Its objects are sets, morphisms are the maps of sets. One has associative composition and units id_x that are the identity maps.

1.6.2. *Example: modules over a ring.* Similarly, k is a field, one defines the category $\mathtt{Vec}_k$ of vector spaces over k. Its objects are vector spaces and morphisms are just linear transformations. More generally, if A is an associative ring, one can define ${}_A\mathtt{Mod}$ — the category of left A-modules, whose objects are left A-modules and morphisms are A-module homomorphisms. We can also define $\mathtt{Mod}_A$, the category of right A-modules.

1.6.3. *Example: topological spaces.* The category `Top` has topological spaces as objects, and continuous maps as morphisms.

1.6.4. *Functors.* A category is a (sort of) mathematical object. There is an appropriate notion of "morphism" from one category to another.

Definition. Let $\mathcal{C}$, $\mathcal{D}$ be two categories. A functor $F : \mathcal{C} \to \mathcal{D}$ consists of

- For each $x \in \mathrm{Ob}(\mathcal{C})$, an object $F(x)$ in $\mathcal{D}$.
- For each pair of objects x, y of $\mathcal{C}$, a map $F : \mathrm{Hom}_{\mathcal{C}}(x, y) \to \mathrm{Hom}_{\mathcal{D}}(F(x), F(y))$.
- One requires $F(\mathrm{id}_x) = \mathrm{id}_{F(x)}$ and $F(gf) = F(g)F(f)$.

1.6.5. *Examples of functors.*

- The functors $\mathtt{Vec}_k \to \mathtt{Set}$, $\mathtt{Top} \to \mathtt{Set}$, ${}_A\mathtt{Mod} \to \mathtt{Set}$ forgetting the structure of a vector space, topological space or A-module.
- The functor $F : \mathtt{Set} \to {}_A\,\mathtt{Mod}$ assigning to a set X the free A-module spanned by X.

1.6.6. *Exercise.* Give more examples of functors.

1.6.7. *Opposite category.* If $\mathcal{C}$ is a category, the opposite category $\mathcal{C}^{\mathrm{op}}$ is defined as follows: it has the same objects, but $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(x, y) = \mathrm{Hom}_{\mathcal{C}}(y, x)$. Composition is defined by an obvious formula.

A functor $F : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ is sometimes called *a contravariant functor* from $\mathcal{C}$ to $\mathcal{D}$.

1.6.8. *Functor* Hom. Given two A-modules X and Y, we want to assign an abelian group $\mathrm{Hom}(X, Y)$. We can easily see that, for fixed X, this is a functor

$$\mathrm{Hom}_A(X, \_) :{}_A\,\mathtt{Mod} \to \mathtt{Ab}.$$

in fact, any homomorphism $f : Y \to Y'$ defines a homomorphism of abelian groups $\mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X, Y')$.

If we fix Y, we can define another functor, now from ${}_A\mathtt{Mod}^{\mathrm{op}}$ to $\mathtt{Ab}$: it carries X to $\mathrm{Hom}_A(X, Y)$ and a homomorhism $f : X \to X'$ to a homomorphism $\mathrm{Hom}_A(X', Y) \to \mathrm{Hom}_A(X, Y)$ (pay attention to the reversion of the arrows!)

We can do even more, considering Hom_A as a functor from ${}_A\mathtt{Mod}^{\mathrm{op}} \times_A \mathtt{Mod}$ to $\mathtt{Ab}$.

To do this, one has to define a product of categories; please do it as an exercise.

1.7. **Properties of the functor** Hom**.**

1.7.1. *Additivity.* This is the property saying that $F(f + g) = F(f) + F(g)$. Of course, it only makes sense when $\mathrm{Hom}_{\mathcal{C}}(x, y)$ and $\mathrm{Hom}_{\mathcal{D}}(x, y)$ are abelian groups (as in our examples).

1.7.2. *Aditivity — 2.* Another property (it actually follows from the previous one, but it is not that obvious) says that F preserves direct sums. We know that $\mathrm{Hom}(X_1 \oplus X_2, Y) = \mathrm{Hom}(X_1, Y) \oplus \mathrm{Hom}(X_2, Y)$ in the sense that there is a canonical isomorphism between two abelian groups. Actually, the claim is even more precise, but we are not yet ready to formulate it, see 1.8.

1.7.3. *Left exactness.* This is what we are going to prove. Let

$$0 \to Y' \xrightarrow{f} Y \xrightarrow{g} Y''$$

be an exact sequence. This means that f is mono, and $\mathrm{Ker}(g) = \mathrm{Im}(f)$.

We have a sequence of abelian groups and homomorphisms

$$0 \to \mathrm{Hom}_A(X, Y') \to \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X, Y''). \tag{1}$$

Proposition. *The sequence (1) is exact.*

Note: pay attention that the exact sequence above does not end with zero!

Proof. First of all, (1) is a complex: a composition of two consecutive arrows is zero. This is something we get "for free": just because an additive functor carries zero morphism to zero.

Let us prove that the first morphism in (1) is mono. This is quite obvious: it carries $\phi : X \to Y'$ to the composition $X \xrightarrow{\phi} Y' \xrightarrow{f} Y$. If the composition is zero, $\phi = 0$ as f is mono.

Let us now prove the exactness in the middle. Assume that for $\phi : X \to Y$ the composition $g \circ \phi$ is zero. This means that for any $x \in X$ the image $\phi(x)$ belongs to the kernel of g. Since $\mathrm{Ker}(g) = \mathrm{Im}(f)$, $\phi(x) \in \mathrm{Im}(f)$. Since f is mono, there is a *unique* element $y' \in Y$ such that $\phi(x) = f(y')$. We define $\psi : X \to Y'$ by the formula $\psi(x) = y'$. We have verify that ψ is a homomorphism of A-modules; this is an easy exercise (DO IT!)

This proves the result: any ϕ in the kernel of the second homomorphism is in the image of the first. □

1.7.4. *Left exactness — 2.* Let

$$X' \xrightarrow{f} X \xrightarrow{g} X'' \to 0$$

be an exact sequence. This means that g is epi, and $\mathrm{Ker}(g) = \mathrm{Im}(f)$.

We have a sequence of abelian groups and homomorphisms

$$0 \to \mathrm{Hom}_A(X'', Y) \to \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X', Y). \tag{2}$$

Proposition. *The sequence (2) is exact.*

Proof. As before, (2) is a complex.

Let us prove that the first morphism in (2) is mono. This is quite obvious: it carries $\phi : X'' \to Y$ to the composition $X \xrightarrow{g} X'' \xrightarrow{\phi} Y$. If the composition is zero, $\phi = 0$ as g is epi.

Let us now prove the exactness in the middle. Assume that for $\phi : X \to Y$ the composition $\phi \circ f$ is zero. This means that $\mathrm{Im}(f) \subset \mathrm{Ker}(\phi)$. Since $\mathrm{Ker}(g) = \mathrm{Im}(f)$, $\mathrm{Ker}(g) \subset \mathrm{Ker}(\phi)$, so by Isomorphism theorem the map ϕ uniquely factors as

$$X \xrightarrow{g} X'' \xrightarrow{\bar{\phi}} Y.$$

This precisely means that ϕ is the image of $\bar{\phi}$.

This proves the result: any ϕ in the kernel of the second homomorphism is in the image of the first. $\square$

1.8. **Direct sum: a second look.** Let M, N be A-modules. Let $X = M \oplus N$. The arrows in the diagram

$$M \underset{p_1}{\overset{i_1}{\rightleftarrows}} X \underset{p_2}{\overset{i_2}{\leftrightarrows}} N \tag{3}$$

are defined by the formulas

$$i_1(x) = (x, 0),\ i_2(y) = (0, y),\ p_1(x, y) = x,\ p_2(x, y) = y. \tag{4}$$

Note that the maps i_1, i_2, p_1, p_2 satisfy the following identities.

$$p_1 i_1 = \mathrm{id}_M,\ p_2 i_2 = \mathrm{id}_N,\ p_2 i_1 = 0 = p_1 i_2,\ i_1 p_1 + i_2 p_2 = \mathrm{id}_X. \tag{5}$$

Vice versa, given a diagram (4) satisfying the conditions (5), the module X uniquely identifies with the direct sum of M and N: in fact, any $x \in X$ has a unique presentation as $x = i_1(p_1(x)) + i_2(p_2(x))$. This strange description of direct sum (by the diagram (4) rather then as a set of pairs) is very convenient if we want to understand what happens to direct sum after an application of a functor: any additive functor in the sense of definition 1.7.1 preserves direct sums. In fact, it carries diagrams (4) satisfying (5) to a diagram with the same property.

In particular, the functor Hom preserves direct sums in both arguments. This is a more detailed explanation of 1.7.2.

1.9. **Exact functors.** An additive functor $F : \mathcal{C} \to \mathcal{D}$ (we assume $\mathcal{C}, \mathcal{D}$ to be categories of modules, so that $\mathrm{Hom}(x, y)$ is always an abelian group) is called exact if it carries any exact sequence

$$\to X_{n+1} \to X_n \overset{d_n}{\to} X_{n-1} \to \tag{6}$$

to an exact sequence.

1.9.1. **Lemma.** *A functor F is exact if and only if it carries any short exact sequence into a short exact sequence.*

Proof. The only if part is clear. We have to show that if short exact sequences are preserves, any exact sequences are preserved. Here is the trick. Given a complex (6), we can "cut" it into a number of short complexes as follows.

$$0 \to \mathrm{Im}(d_{n+1}) \overset{i_n}{\to} X_n \overset{p_n}{\to} \mathrm{Im}(d_n) \to 0. \tag{7}$$

Vice versa, given a collection of complexes (7), we reconstruct the complex (6) defining the maps $d_n : X_n \to X_{n-1}$ as the composition $d_n = i_{n-1} \circ p_n$.

Note that if the complex (6) is exact, the complexes (7) are short exact sequences, and vice versa, if (7) are short exact, then (6) is exact. This reduces the preservation of exact sequences to short exact sequences. □

1.10. **Projective modules.** The functor $\mathrm{Hom}_A(M, \_)$ is left exact. We now want to know conditions for M for which it is exact.

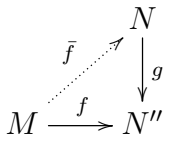
If $0 \to N' \to N \to N'' \to 0$ is a short exact sequence, we have an exact sequence

$$0 \to \mathrm{Hom}_A(M, N') \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'').$$

the only condition we have to add is that the last arrow is surjective.

1.10.1. **Definition.** An A-module M is projective if for any epimorphism $N \to N''$ the map $\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'')$ is an epimorphism. Equivalently, M is projective if for any pair of arrows f, g with g surjective there exists $\bar{f}$ making the diagram commutative (that is, satisfying $g \circ \bar{f} = f$).

(8)



It turns out that there is an easy description of projective modules (it is not very explicit, though).

First of all, one has the following.

1.10.2. **Lemma.** *Any free A-module is projective.*

Proof. This is an easy exercise. Let in the above diagram $M = F(X)$ is free generated by a set X. In order to define $\bar{f} : F(X) \to N$, it is sufficient to define any map $X \to N$, with the only condition that its composition with g gives f. This can be done separately for every $x \in X$ (using an axiom of choice) as g is surjective. □

1.10.3. **Proposition.** *An A-module P is projective iff there is a module Q such that $P \oplus Q$ is free.*

Proof. Let $N \to N''$ be surjective. If $P \oplus Q$ is free, the map $\mathrm{Hom}_A(P \oplus Q, N) \to \mathrm{Hom}_A(P \oplus Q, N'')$ is surjective. It can be described as the sum of two maps, $\mathrm{Hom}_A(P, N) \to \mathrm{Hom}_A(P, N'')$ and $\mathrm{Hom}_A(Q, N) \to \mathrm{Hom}_A(Q, N'')$. Therefore, each of them is also surjective.

In the opposite direction, let P be projective. We can find a free module F and an epimorphism $g : F \to P$. Then the map $f := \mathrm{id} : P \to P$ can be lifted to $\bar{f} : P \to F$, so that $g \circ \bar{f} = \mathrm{id}_P$. This means that P is a direct summand of F. □

Description of projective modules is sometimes an interesting problem. Sometimes it is easy. For instance, any projective $\mathbb{Z}$-module is free (that is, a free abelian group). This follows from the following more general result.

1.10.4. **Theorem.** *Any subgroup of a free abelian group is free.*

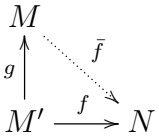
Proof. We will ony prove the claim for finitely generated abelian groups. The general result is also correct, but the proof requires Zorn lemma, see [L], App. 2.

Let F be a free abelian group generated by $x_1, \dots, x_n$ and let $P \subset F$. We define $F_k = \mathrm{Span}_{\mathbb{Z}}(x_1, \dots, x_k)$ and $P_k = P \cap F_k$. We will prove by induction that P_k is free abelian group of rank $\leq k$. For $k = 1$ this is clear as P_1 is isomorphic to a subgroup of $\mathbb{Z}$. Assume by induction that P_{k-1} is free of rank $\leq k-1$. If $P_k = P_{k-1}$, there is nothing to prove. Otherwise, there exists $x \in P_k$, $x = \sum_{i=1}^{k} a_i x_i$, such that $a_k \neq 0$. Let us choose an element x having a minimal possible value of $|a_k|$. We claim that $P_k = P_{k-1} \oplus \mathrm{Span}_{\mathbb{Z}}(x)$. In fact, the intersection $P_{k-1} \cap \mathbb{Z} \cdot x$ is obviously zero. On the other hand, if $y \in P_k$ has form $y = \sum_{i=1}^{k} b_i x_i$, b_k should be divisible at a_k (otherwise some $y - cx$ will have a smaller coefficient of x_k), say, $b_k = ca_k$, which implies that $y - cx \in P_{k-1}$. $\square$

1.11. **Injective modules.** One can formally do the same thing with the functor $F = \mathrm{Hom}_A(\_, N)$. It is always left exact, and we would like to know for which A-modules N is it exact. We get the following definition.

1.11.1. **Definition.** An A-module N is injective if for any monomorphism $M' \to M$ the map $\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N)$ is an epimorphism. Equivalently, N is injective if for any injective $g : M' \to M$, any $f : M' \to N$ can be extended to $\bar{f} : M \to N$.

(9)



There are no obvious examples of injective modules.

The folloowing result allows one to simplify the verification of injectivity.

1.11.2. **Lemma.** *A left A-module N is injective iff for each left ideal $I \subset A$ and for any $f : I \to N$ homomorphism of A-modules there exists $x \in N$ such that $f(a) = ax$.*

Proof. If N is injective, f can be extended to a homomorpism $\bar{f} : A \to N$ which is uniquely given by $x = \bar{f}(1)$. Then $\bar{f}(a) = ax$.

The other implication is slightly less trivial. Let $g : M' \to M$ be monomorphism and $f : M' \to N$ be given. We will use Zorn lemma to extend f "as much as possible". Then we will prove that we extended it to the whole of M. This is done as follows.

Define the following poset (=partially ordered set) X. An element of X is a pair $(K, \phi : K \to N)$ where K is a submodule of M containing $g(M')$ and $\phi \circ g = f$. The order on X is very natural: $(K, \phi) \leq (K', \phi')$ if $K \subset K'$ and $\phi = \phi'|_K$.

It is standard to verify that the condition of Zorn lemma is fulfilled. Therefore, there is a maximal element (K, ϕ) in X. It remains to prove that $K = M$. If not, there is $x \in M \setminus K$. Denote $K' = F + Ax$. We will show that in this case the map $\phi : K \to N$ extends to $\phi' : K' \to N$. In fact, a map ϕ' is uniquely given by its restriction $\phi : K \to N$ and by $y = \phi(x)$, with the condition that these two maps ϕ and $Ax \to N$ coincide at the intersection. Let $I = \{a \in A | ax \in K\}$. This is a left ideal in A and $\phi : K \to N$ defines a homomorphism $\alpha : I \to N$ by the formula $\alpha(i) = \phi(ix)$. By the assumption, there exists $y \in N$ such that $\alpha(i) = iy$. This means that the map $\phi' : K' \to N$ can be defined by the formula $\phi'|_K = \phi$, $\phi'(x) = y$. This proves that our assumption $K \neq M$ cannot possibly hold. □

We can now describe injective abelian groups.

1.11.3. **Definition.** N is divisible if for any $x \in N$ and for any nonzero integer n there exists $y \in N$ such that $x = ny$.

1.11.4. **Theorem.** *An abelian group is injective iff it is divisible.*

This is now an exercise.

1.11.5. *Projective resolutions.* Any A-module M can be presented as an image of a projective A-module: we can, for instance, present M as an image of a free A-module, to get

$$P \xrightarrow{f} M \to 0.$$

If $A = \mathbb{Z}$ (or any PID, principal ideal domain, see Homework 2), $\mathrm{Ker}(f) \subset P$ is also free, so, any A-module M can be presented by a short exact sequence

$$0 \to P_1 \to P_0 \to M \to 0,$$

where P_i are projective. Such exact sequence is called a *projective resolution* of M and we say that any module over a PID has a projective resolution of length ≤ 1.

Projective modules have a projective resolution of length 0, so the minimal length of a projective resolution can serve as a measure of "non-projectivity" of a module.

There is a similar story about injectivity, and we will now explain it. The main important fact here is that any module can be embedded into an injective module. ONce we know this, we can repeat the above story about projective resolutions, inverting all arrows and replacing projective modules with injective modules. Details are in the next subsection.

1.12. **Injective modules, 2.**

1.12.1. *Direct sum and direct product.* For two modules M, N there is no difference between direct sum and direct product.

We will now explain the difference, when the number of factors / summands is infinite. We start with an explicit construction.

Let M_i, $i \in I$, be a collection of modules.

Definition. Direct product $\prod_{i\in I} M_i$ is defined as the cartesian product (as a set), endowed with the componentwise operations: $(x_i) + (y_i) = (z_i)$ with $z_i = x_i + y_i$, and $a(x_i) = (ax_i)$.

Definition. Direct sum $\oplus_{i\in I} M_i$ is the submodule of $\prod_{i\in I} M_i$ consisting of the collections (x_i) such that only finite number of x_i is nonzero.

At the moment, the definitions look strange, but we will explain what is going on.

First of all, one has projection maps $p_i : \prod M_i \to M_i$ and injection maps $r_i : M_i \to \oplus M_i$.

(of course we can compose these maps with the embedding $\oplus M_i \to \prod M_i$ and get $p_i' : \oplus M_i \to M_i$ and $r_i' : M_i \to \prod M_i$, but the maps p_i' and r_i' will not satisfy the very important properties we will now formulate.

The properties of direct product and direct sum are categorical in nature, that is, make sense for any category.

The property of $\prod M_i$ is that, a map $f : X \to \prod M_i$ is uniquely defined by its compositions $p_i \circ f : X \to M_i$. Formally, for any X the map

$$\mathrm{Hom}(X, \prod M_i) \to \prod \mathrm{Hom}(X, M_i) \tag{10}$$

carrying $f : X \to \prod M_i$ to $(p_i \circ f)$, is a bijection.

Note that the product on the right is the usual cartesian product of sets.

The property of direct sum is, in a sense, dual.

It says that a map $f : \oplus M_i \to Y$ is uniquely defined by the compositions $f \circ r_i : M_i \to Y$. Formally, that for any Y the map

$$\mathrm{Hom}(\oplus M_i, Y) \to \prod \mathrm{Hom}(M_i, Y) \tag{11}$$

carrying $f : \oplus M_i \to Y$ to $(f \circ r_i)$, is a bijection.

One has to think a little bit to see the difference. If we have a collection of maps $f_i : M_i \to Y$, we will define the corresponding map $f : \oplus M_i \to Y$ as the one carrying (x_i) to $\sum f_i(x_i)$. Note that in order to be able to calculate the sum, it has to be finite!

As an easy result of the above definition, we have

1.12.2. **Lemma.** 1. *One has*

$$\mathrm{Hom}_A(\oplus M_i, N) = \prod \mathrm{Hom}_A(M_i, N).$$

2. *One has*
$$\mathrm{Hom}_A(M, \prod N_i) = \prod \mathrm{Hom}_A(M, N_i).$$

□

And an easy corollary of the above formula.

1.12.3. **Proposition.** 1. *If P_i are projective, $\oplus P_i$ is also projective.*
2. *If J_i are injective, $\prod J_i$ is also injective.*

Proof. One has $\mathrm{Hom}(\oplus P_i, N) = \prod \mathrm{Hom}(P_i, N)$. Direct product of a collection of epimorohisms is an epimorphism. The same reasoning proves the second claim. □

We are now back to studying injective modules.

1.12.4. *Abelian groups.* We will first prove that any abelian group N can be embedded into a divisible group.

Proposition. *For any abelian group N there exists a monomorphism $N \to J$ into a divisible group J.*

Proof. First of all, if G is a divisible group then any factor G/H is divisible (explain this!). The group $\mathbb{Q}$ is clearly divisible, so $\mathbb{Q}/\mathbb{Z}$ is also divisible.

For any abelian group G we define $G^\vee = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. If $G = F(X)$, $G^\vee = \prod_{x \in X} \mathrm{Hom}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = \prod_{x \in X} \mathbb{Q}/\mathbb{Z}$ is injective.

In general there is an epimorphism $F \to G \to 0$, so an exact sequence $0 \to G^\vee \to F^\vee$. Thus, $G^\vee$ embeds into a divisible group.

It remains to note that there is a natural map $i : G \to (G^\vee)^\vee$ defined, as for vector spaces, by the formula $(x \in G, \phi \in G^\vee)\ i(x)(\phi) = \phi(x)$. Let us show i is injective. If $i(x) = 0$, all homomorphisms $\phi : G \to \mathbb{Q}/\mathbb{Z}$ carry x to 0. Assume $x \neq 0$.

Look at the subgroup H of G generated by x. This is a cyclic group and there is a nonzero homomorphism $f : H \to \mathbb{Q}/\mathbb{Z}$.

(in fact, if H is an infinite cyclic group, any nonzero choice for $f(x) \in \mathbb{Q}/\mathbb{Z}$ gives a nonzero homomorphism $H \to \mathbb{Q}/\mathbb{Z}$. Otherwise, if $ord(x) = n$, we can define $f(x) = \frac{1}{n} + \mathbb{Z}$).

Now, since $\mathbb{Q}/\mathbb{Z}$ is injective, f can be extended to a homomorphism $\bar{f} : G \to \mathbb{Q}/\mathbb{Z}$. It cannot be zero as its restriction f is nonzero. Contradiction.

Finally, G embeds into $(G^\vee)^\vee$ which embeds into a divisible group. □

1.12.5. *Over any ring A.* We will now deduce the existence of embedding of an arbitrary A-module into an injective module from the similar result for abelian groups.

The main tool for doing this is a functor from abelian groups to A-modules defined as follows.

Let T be an abelian group. Look at the abelian group $\mathrm{Hom}_{\mathbb{Z}}(A,T)$. We can convert it into a left A-module as follows. Let $a \in A$ and $f \in \mathrm{Hom}(A,T)$. we define $af : A \to T$ by the formula $(af)(b) = f(ba)$. It is an easy exercise to verify that this formula defines a left A-module $\mathrm{Hom}_{\mathbb{Z}}(A,T)$. This is definitely a functor $\mathtt{Ab} \to_A \mathtt{Mod}$. We will show that this functor preserves injective modules: it carries divisible groups to injective A-modules. To verify this, we need a nice formula for the group of A-homomorphisms $\mathrm{Hom}_A(X, \mathrm{Hom}_{\mathbb{Z}}(A,T))$. It is given by the following lemma.

Lemma. *One has a natural isomorphism of abelian groups*

$$\theta : \mathrm{Hom}_A(X, \mathrm{Hom}_{\mathbb{Z}}(A,T)) \to \mathrm{Hom}_{\mathbb{Z}}(X,T). \tag{12}$$

Proof. We will present the isomorphism. Then we will comment what does the word "natural" mean in the formulation of the lemma.

Any A-linear map $f : X \to \mathrm{Hom}_{\mathbb{Z}}(A,T))$ allows one to construct a $\mathbb{Z}$-linear map $\phi : X \to T$ by the formula $\phi(x) = (f(x))(1)$: $f(x)$ is a map $A \to T$, and we evaluate it at $1 \in A$. Vice versa, any $\mathbb{Z}$-linear map $\phi : X \to T$ defines $f : X \to \mathrm{Hom}_{\mathbb{Z}}(A,T)$ by the formula

$$f(x)(a) = \phi(ax).$$

It is easy to verify that the constructions above are mutually invervse.

Now, a comment about the meaning of the word "natural". Both expressions, $\mathrm{Hom}_A(X, \mathrm{Hom}_{\mathbb{Z}}(A,T))$ and $\mathrm{Hom}_{\mathbb{Z}}(X,T)$ are functor in two arguments, $X \in_A \mathtt{Mod}$ and $T \in \mathtt{Ab}$ (contravariant in X). Naturality of the isomorphism means that for different values of X and T the respective isomorphisms are compatible.

In more detail, let $f : X \to Y$ be a homomorphism of A-modules. Then we have a diagram of abelian groups presented below.

$$\begin{array}{ccc} \mathrm{Hom}_A(X, \mathrm{Hom}_{\mathbb{Z}}(A,T)) & \xrightarrow{\theta} & \mathrm{Hom}_{\mathbb{Z}}(X,T) \\ {\scriptstyle f^*}\uparrow & & \uparrow{\scriptstyle f^*} \\ \mathrm{Hom}_A(Y, \mathrm{Hom}_{\mathbb{Z}}(A,T)) & \xrightarrow{\theta} & \mathrm{Hom}_{\mathbb{Z}}(Y,T) \end{array} \tag{13}$$

The "naturality" means that this diagram is commutative: different θ's are compatible with variation of the "parameters" X and T. Commutativity of the diagram has to be verified (but the verification is very easy, it is left as an exercise).

1.12.6. *Naturality, in general.* Here is the general picture. We have two categories, $\mathcal{C}$ and $\mathcal{D}$, and two functors $F, G : \mathcal{C} \to \mathcal{D}$.

A morphism $\alpha : F \to G$ of functors is the collection of morphisms $\alpha(x) : F(x) \to G(x)$ in $\mathcal{D}$ for each $x \in \mathrm{Ob}(\mathcal{C})$, satisfying the following condition.

For each $f : x \to y$ in $\mathcal{C}$ the diagram

$$\begin{array}{ccc} F(x) & \xrightarrow{\alpha(x)} & G(x) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(y) & \xrightarrow{\alpha(y)} & G(y) \end{array} \tag{14}$$

is commutative.

Obviously, naturality of the isomorphism θ in the lemma is a special case of the above definition.

This is an isomorphism of two functors: $\mathrm{Hom}_A(\_, \mathrm{Hom}_{\mathbb{Z}}(A, T))$ and $\mathrm{Hom}_{\mathbb{Z}}(\_, T)$.

1.12.7. *The end of the construction.* Recall that or aim is to construct, for any A-module M, an embedding $M \to J$ into an injective A-module. Here is what we do. Look at M as an abelian group. Let $\phi : M \to T$ be an embedding of M into a divisible group T. According to the lemma, we deduce from this embedding a map of A-modules $f : M \to \mathrm{Hom}_{\mathbb{Z}}(A, T)$. We will verify that f is also an embedding and $\mathrm{Hom}_{\mathbb{Z}}(A, T)$ is an injective A-module. The first claim is very easy: if $f(x) = 0$ then $f(x)(1) = 0$, that is $\phi(x)$=0. Since ϕ is injective, f is injective.

The second claim is also very easy. We have to verify that the functor $\mathrm{Hom}_A(\_, \mathrm{Hom}_{\mathbb{Z}}(A, T))$ is exact. The lemma says that this functor is isomorphic to $\mathrm{Hom}_{\mathbb{Z}}(\_, T)$ which is exact as T is an injective $\mathbb{Z}$-module.

□

2. Rings, modules, II

The topics we will study here include:

- Finitely generated modules over PID.
- Finite length modules in general.
- Tensor product of modules.

2.1. **Modules over PID.** Semisimple rings have a simplest possible category of modules: there is a finite number of isomorphism classes of simple modules, and any module is a direct sume of these. Complete description of modules is seldom possible. We will now study the next class of rings where it is possible to describe all finitely generated modules. These are PID — principal ideal domains. The examples of PID include

- $\mathbb{Z}$.
- $k[x]$ where k is a field.
- $\mathbb{Z}[i]$, the ring of Gaussian numbers — these are complex numbers $a + bi$ with $a, b \in \mathbb{Z}$.

A special case of the theorem we are going to prove we know from Linear algebra — this is the theorem on Jordan form of a matrix. We will start with reformulating this Linear algebra theorem in our language.

2.1.1. *Jordan normal form.* Let k be an algebraically closed field, V a finitely dimensional vector space over k and let $T : V \to V$ be a linear operator. The pair (V, T) determines on V a structure of $k[x]$ modules, where x acts on V as the operator T.

Thus, the classification of pairs (V, T) is the same as the classification of $k[x]$-modules that are finite-dimensional as k-vector spaces.

Jordan normal form is a presentation of (V, T) in a standard form — as a direct sum of "Jordan blocks", where a Jordan block of size n with the eigenvalue λ (we will denote it $J_n(\lambda)$) is the vector space with the basis $e_1, \dots, e_n$, and with the operator T givem by the formulas

$$T(e_1) = \lambda e_1,\ T(e_k) = e_{k-1} + \lambda e_k\ (k > 1).$$

Let us describe the $k[x]$-module $J_n(\lambda)$. It is generated by one element e_n (verify this!) so it has form $k[x]/I$ where I is the set of polynomials annihilating e_n. It is easy to see (verify this!) that I is generated by the polynomial $(x - \lambda)^n$. This gives the following reformulation of the classical theorem.

Theorem. *(Jordan normal form) Let k be an algebraically closed field and $T : V \to V$ and endomorphism of a finite-dimensional vector space V. Then (V, T) considered as a $k[x]$-module is isomorphic to a direct sum*

$$k[x]/((x - \lambda_1)^{m_1}) \oplus \dots \oplus k[x]/((x - \lambda_k)^{m_k}).$$

2.1.2. *PID: basis facts.* Recall that a ring A is called PID if it satisfies the following properties.

- It is a commutative domain (that is, has no zero divisors).
- Any ideal in A is principal (that is, of the form (a) for some $a \in A$.

An element $p \neq 0$ is called prime if it is not invertible and if $p = ab$ implies a or b is invertible.

If A is a PID, any nonzero element in it has a unique (up to obvious ambiguity) decomposition as a product of primes.

If A has no primes, A is a field.

Note

Lemma. *Let I be an ideal in A and let $\rho : A \to A/I$ be the natural homomorphism. Then, for any proper ideal K in A/I the preimage $J = \rho^{-1}(K)$ is a proper ideal in A and $K = \rho(J)$.*

Proof. Obviously $\rho(J) \subset K$. Since ρ is surjective, for any element $x \in K$ the preimage $\rho^{-1}(x)$ is nonempty. If $J = A$, $\rho(J) = A/I$. □

Lemma. *Let A be PID that is not a field, p a prime element of A. Then $A/(p)$ is a field.*

Proof. We will prove that $A/(p)$ has no nonzero nontrivial ideals. If K is a nonzero nontrivial ideal in $A/(p)$ then its preimage J in A is nontrivial, so $J = (x)$ where x is not invertible. $x \notin (p)$ as otherwise its image K would be zero. Obviously, $(x) \supset (p)$ so $p = xy$ is a nontrivial decomposition of p — contradiction. □

We will now formulate the main result we want to prove.

2.1.3. **Theorem.** *Let A be a PID. Any finitely generated A-module M can be presented*

$$M = F \oplus A/(p_1^{m_1}) \oplus \ldots \oplus A/(p_k^{m_k}),$$

where F is a free A-module of finite rank. The rank of F, as well as the elements p_i and the powers m_i are uniquely defined.

Remark: as usual, p_i are uniquely defined up to invertible and up to reordering.

2.1.4. *Applications.* The first application is Jordan normal form, see above. Here is another one.

Corollary. *Any finitely generated abelian group can be pre sented as a direct sum*

$$A = F \oplus \mathbb{Z}/p_1^{m_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_k^{m_k}\mathbb{Z}.$$

The rank of F, as well as the collection of numbers p_i (primes) and m_i is uniquely defined by A.

2.2. The proof of the theorem.

2.2.1. *Torsion part.* Let M be an A-module, when A is an integral domain. We denote $M^t = \{x \in M | \exists a \neq 0 : ax = 0\}$. This is *the torsion part* of M.

It is obvious M^t is a submodule of M.

Lemma. *The quotient M/M^t has no torsion.*

Proof. Let $x \in M$ such that the image of x is M/M^t is a torsion element. This means that for some $a \neq 0$ $ax \in M^t$ so for some $b \neq 0$ $abx = 0$. Since A has no zero divisors, $ab \neq 0$ and so x is a torsion element. □

From now on A is PID. We will prove later that

- A submodule of a finitely generated module is finitely generated. This will imply that M^t is f.g.
- Any f.g. module without torsion is free. This will imply that M is isomorphic to a direct sum of M^t and the free module M/M^t.

This will divide the classification problem into two: uniqueness of rank of a free A-module (this has place over any commutative ring), and description of f.g. torsion modules.

First of all, let us carefully define the rank of a free module.

2.2.2. **Definition.** Let F be a free module generated by a set X. Rank of F is, by definition, the cardinality of X.

It is not immediately clear that a free module has uniqely defined rank. We will show this now for PID. Almost the same proof will work for any commutative ring (this will be an exercise).

2.2.3. **Lemma.** *Let $F(X)$ and $F(Y)$ be isomorphic free A-modules, where A is a PID. Then $|X| = |Y|$.*

Proof. If A is a field, this is a standard fact of Linear algebra (notion of dimension of a vector space).

If not, any A-module M defines $A/(p)$-module M/pM. If M is free with a basis X, M/pM will be a free $A/(p)$-module with the same basis. This reduces the claim to the case A is a field. □

The following result has already been proven for $A = \mathbb{Z}$ and given as a homework for a general PID.

2.2.4. **Lemma.** *Let M be a submodule of a free A-module F of rank k. Then M is free of rank $\leq k$.*

2.2.5. **Corollary.**

- *A factor of a finitely generated module is finitely generated.*
- *Let A be PID. Then any submodule of a finitely generated module is finitely generated.*

Proof. The first claim is obvious: If X spans M, the images of X in M/N span M/N. Let us prove the second claim. If M is f.g., one can present M as the image of $F(X)$ where X is a finite set. If $N \subset M$, let $\tilde{N} \subset F(X)$ be the preimage of N. Then $\tilde{N}$ is finitely generated free, and N is finitely generated as a quotient of $\tilde{N}$. □

2.2.6. **Proposition.** *Let M be a torsion-free f.g. A-module. Then M is free.*

Proof. Let $\{x_1, \dots, x_n\}$ be a finite set generating M and let $\{y_1, \dots, y_m\}$ be a maximal subset of $\{x_i\}$ which is independent over A. For each $k = 1, \dots, n$ x_k cannot be added to $\{y_j\}$, so there is a linear dependence

$$a_k x_k + \sum b_j y_j = 0$$

that is, $a_k x_k \in F := \mathrm{Span}_{\mathbb{Z}}(y_1, \dots, y_m)$. Put $a = \prod a_k$. We get $a x_k \in F$. This means that multiplication by $a \in \mathbb{Z}$ defines a monomorphism $M \to F$. Thus, M is isomorphic to a submodule of F and is, therefore, free. □

We now have a surjective map $M \to M/M^t$ with M/M^t free. We know that each surjective map to a free module splits. Therefore, there is an isomorphism $M = M^t \oplus F$ where $F = M/M^t$ is a free module (of finite rank).

We now reduced everything to the study of f.g. torsion modules.

2.3. **Finitely generated torsion modules.** In this subsection A is a PID.

Note that torsion modules are not necessarily finitely generated (exercise: give an example).

Let M be a f.g. torsion module. If M is generated by $x_1, \dots, x_n$, and $a_k x_k = 0$ (all elements are torsion elements) then for $a = \prod a_k$ we have $ax_k = 0$ so $aM = 0$. Thus, any torsion f.g. module is annihilated by a nonzero element. We can define $I = \{a \in A | aM = 0\}$. This is a nonzero ideal in A, so it is generated by one element. Let $I = (a)$, so that $a \in A$ is "the smallest" element annihilating M.

One has a unique decomposition $a = u \prod_{i=1}^n p_i^{m_i}$ where u is invertibe and p_i are different primes in A.

For any prime p we define

$$M(p) = \{x \in M | \exists n : p^n x = 0\}.$$

2.3.1. **Proposition.** 1. *For any prime $p \in A$ $M(p) = 0$ if $p \not| a$.*

2. *$M(p_i) = \{x \in M | p_i^{m_i} x = 0\}$.*

3. *$M = M(p_1) \oplus \dots \oplus M(p_n)$.*

This proposition reduces the general case to the case M is annihilated by a power of p.

Proof. 1. If $p \not| a$ and $x \in M(p)$ then $p^k x = 0$, so, if y denotes the last nonzero element in the sequence

$$x, px, \dots, p^k x,$$

$py = 0$ as well as $ay = 0$, so $\gcd(p, a)y = 0$ that is $y = 0$. Contradiction.

2. We have to verify that, if for some m $p_i^m x = 0$ than $p_i^{m_i} x = 0$. This follows from the fact that $\gcd(a, p_i^m) = p_i^{m_i}$.

3. For any $q \in A$ (not necessarily prime!) we defnie $M_q = \{x \in M | qx = 0\}$. We have $M = M_a$. We will now verify that, if $a = bc$ with $gcd(b, c) = 1$, then $M_a = M_b \oplus M_c$. This will imply by induction that $M = M_{p_1^{m_1}} \oplus \dots \oplus M_{p_n^{m_n}}$.

In fact, there exist $r, s \in A$ such that $rb + sc = 1$. Then any $x \in M$ decomposes as $x = rbx + scx$ where $rbx \in M_c$ and $scx \in M_b$. This implies that $M_a = M_b + M_c$. The intersection is obviously zero as b, c are coprime. This proves the claim. $\square$

Our final step is decomposition of a single $M(p) = M_{p^m}$ for $p = p_i$ for some i.

2.3.2. **Proposition.** *Let M be a f.g. A-module annihilated by a power of p. Then M can be presented as a direct sum of cyclic submodules of form $A/(p^r)$ for some r.*

Proof. Let M be generated by $x_1, \dots x_n$. We will prove the claim by induction in n.

We that M is annihilated by p^m where m is minimal possible. This means that all x_i are annihilated by p^m and some of them, say, p_1 is not annihilated by p^{m-1}. We have a short exact sequence

$$0 \to Ax_1 \to M \to N \to 0$$

with $N = M/Ax_1$ generated by the images of $x_2, \dots, x_n$. By induction, N is a direct sum of cyclic submodules, which means that there exist $y_2, \dots, y_t$ such that $N = Ay_2 \oplus \dots \oplus Ay_t$. Let y_j, $j = 2, \dots, t$, be annihilated by p^{m_j} and not by a smaller degree of p. We will find, for each j, a preimage x_j in M satisfying the additional property $p^{m_j}x_j = 0$. This will give (as we will show) a direct decomposition of M.

There is no problem of finding a preimage x'_j of y if we do not require our extra condition: the map $M \to N$ is surjective.

We will now correct x'_j. We will be looking for x_j in the form $x_j = x'_j - cx_1$ where $c \in A$ is the parameter we can play with.

The element x_j has image y_j in N as x_1 is in the kernel. It remains to fit $c \in A$ so that x_j is annihilated by p^{m_j}. Let's do this.

We have $p^{m_j}x'_j$ belongs to the kernel of the epimorphism $M \to N$ as $p^{m_j}y_j = 0$. Therefore, $p^{m_j}x'_j = ax_1$ for some $a \in A$. Since p^m annihilates the whole of M, $0 = p^{m-m_j}p^{m_j}x'_j = p^{m-m_j}ax_1$, therefore, a is divisible by p^{m_j}. We put $c = \frac{a}{p^{m+j}}$ and we are done.

Finally, it is easy to see that the collection of x_j as above provides a splitting of the projection $M \to N$. □

We will now take care of uniqueness.

2.3.3. **Proposition.** *Let A be a PID, M a finitely generated A-module. Then the decomposition*

$$M = F \oplus A/(p_1^{m_1}) \oplus \dots \oplus A/(p_k^{m_k})$$

of M as a direct sum of a free module and of cyclic primary modules is unique in the following sense. Let

$$F \oplus A/(p_1^{m_1}) \oplus \dots \oplus A/(p_k^{m_k}) = F' \oplus A/(q_1^{n_1}) \oplus \dots \oplus A/(q_l^{n_l}). \tag{15}$$

Then F and F' have the same ranks, $k = l$, and, after changing the orders of the summands, $p_i = q_i$ (up to invertible factor) and $m_i = n_i$.

Proof. The torsion pari M^t is uniquely defined, so F and F' are isomorphic as both are isomorphic to M/M^t. Therefore, as we have already proven, their ranks are the same. Furthermore, the decomposition of $M^t = \bigoplus M^t(p)$ is also unique, so everything reduces to the case M is annihilated by a power of a prime p.

Thus, $M = A/(p^{m_1}) \oplus \ldots \oplus A/(p^{m_k})$ is isomorphic to $A/(p^{n_1}) \oplus \ldots \oplus A/(p^{n_l})$, where $m_i \geq 1$ and $n_j \geq 1$, and we have to verify that $k = l$ and the collection of n_i coincides with the collection of m_i. Let us describe $M_p = \{x \in M | px = 0\}$. For the first decomposition we see that $M_p = (A/(p))^k$ and for the second $M_p = (A/(p))^l$. This implies that $k = l$ and alloows us to prove the result by induction: replace M with M/M_p, we will get two decompositions

$$M/M_p = A/(p^{m_1-1}) \oplus \ldots \oplus A/(p^{m_k-1})$$

and

$$M/M_p = A/(p^{n_1-1}) \oplus \ldots \oplus A/(p^{n_l-1}).$$

By induction we may assume that these two decompositions coincide, that is that the nonzero numbers among $m_i - 1$ and $n_j - 1$ coincide. Since we already know that $k = l$, this proves the claim. □

2.4. **Chain conditions.** A module M has *ascending chain condition, a.c.c.* if any ascending chain of submodules

$$M_1 \subset M_2 \subset \ldots$$

stabilizes ($M_k = M_{m+1} = \ldots$).

Another name: noetherian module (Emmi Noether).

A module M has *descending chain condition, d.c.c.* if any descending chain of submodules

$$M_1 \supset M_2 \supset \ldots$$

stabilizes ($M_k = M_{m+1} = \ldots$).

Another name: artinian module (Emil Artin).

All four possibilities are possible for modules: the satisfy both conditions, any one of them and none.

Here are most interesting examples.

2.4.1. $\mathbb{Z}$ as abelian group is noetherian and not artinian.

2.4.2. Look at $H \subset \mathbb{Q}$ consisting of the fractions $\frac{a}{p^n}$ with fixed prime p. Let $G = H/\mathbb{Z}$. This is an abelian group whose all elements have order p^k. One can prove that all nontrivial subgroups of G are of the form $\langle \frac{1}{p^k} \rangle$. This shows that G is artinian but not noetherian.

2.4.3. **Proposition.** *Let*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

be an exact sequence. Then

- *M is noetherian iff M' and M'' are.*
- *M is artinian iff M' and M'' are.*

Proof. The proof is very easy and we will indicate it only for the noetherian property. If M is noetherian, then obviously any ascenting chain of submodules of M' stabilizes, so M' is noetherian. If $\{M''_k\}$ is an ascending chain in M'', the preimages M_k of M''_k form an ascending chain in M. Thus, the chain M_k stabilizes, therefore, M''_k stabilizes.

In the opposite direction, any ascending chain $\{M_k\}$ in M gives rise to two chains, $M'_k = i^{-1}(M_k)$ in M' and $M''_k = p(M_k)$ in M''. If M' and M'' are noetherian, both chains stabilize. Let us show that this implies that the original chain stabilizes. In fact, assume $M'_n = M'_{m+1}$ and $M''_n = M''_{n+1}$. We will show that this implies $M_n = M_{n+1}$. Let $x \in M_{n+1}$. We want to show that $x \in M_n$. Here is what we do. The image $p(x)$ is in $M''_{n+1} = M''_n$, so, there is $y \in M_n$ such that $p(x) = p(y)$. Then $x - y$ belongs to M_{n+1} and to $\mathrm{Ker}(p) = \mathrm{Im}(i)$ so $x - y = i(z)$ with $z \in M'_{n+1} = M'_n$. This means that $i(z) \in M_n$ and then $x = y + z \in M_n$. We are done. □

2.4.4. **Corollary.** *A finite direct sum of noetherian (artinian) modules is noetherian (artinian).*

□

2.4.5. **Proposition.** *A module is noetherian iff any its submodule is finitely generated.*

Proof. Let any submodule of M is f.g. and let $\{M_k\}$ be an ascending chain of submodules. Put $N = \bigcup M_k$. This is a submodule of M, so it is generated by a finite set of elements $x_1, \ldots, x_n$. Each x_i belong to some M_k, so all of them belong to some M_K for K big enough. Then $N = M_K$ and the chain stabilizes.

In the opposite direction, let M be noetherian and let N be a submodule of M. It is also noetherian. Look at the collection $\mathcal{N}$ of all finitely generated submodules of N. It has a maximal element: if there were no one, we could find a sequence $N_1 \subset N_2 \subset \ldots$ of submodules which would not stabilize.

Well, thus, there is N_0 maximal among f.g. submodules of N. If $N_0 \neq N$, choose $x \in N - N_0$. Then $N_0 + Ax$ is a f.g. submodule of N strictly greater than N_0. Contradiction. Thus, $N_0 = N$ and we are done. □

2.4.6. **Definition.**
- A ring is (left or right) noetherian if it is noetherian as a (left or right) module over itself.
- A ring is (left or right) artinian if it is artinian as a (left or right) module over itself.

2.4.7. **Example.**
- A semisimple ring is artinian and noetherian.
- A PID is noetherian but not artinian.
- $k[x_1, x_2, \ldots]$, ring of polynomials of infinite number of generators, is not noetherian.

We will prove later (Hilbert basis theorem) that $k[x_1, \ldots, x_n]$ is noetherian.

Any artinian ring is automatically noetherian. We will probably prove this for commutative rings.

2.4.8. **Proposition.** *Let A be noetherian. Then any f.g. A-module is noetherian.*

Proof. M is f.g, therefore there exists F, f.g. free A-module and a sujective homomorphism $F \to M$. A is noetherian, therefore F is noetherian, hence M is noetherian. □

2.5. **Modules of finite length.** A module M is of finite length if there exists a finite sequence of submodules

$$M = M_0 \supset M_1 \supset \ldots \supset M_n = 0$$

such that all quotients are simple. Such a sequence is called a *composition series*.

The number n in the definition is called *the length of the composition series*.

A module M is called of finite length of it has a composition series.

We will prove that

- Any series of submodules can be completed to a composition series.
- Lengths of all composition series are the same.
- A module is of finite length iff it is both noetherian and artinian.
- Collection of composition factors of a module of finite lenth is independent of the choice of a composition series.

2.5.1. **Proposition.** *Let M have a composition series of length n. Then every composition series has length n and any chain can be completed to a composition series.*

Proof. Let $l(M)$ denote the smallest length of a composition series (or ∞ if there is no composition series). Then one has the following.

- $N \subset M$ implies $l(N) < l(M)$. In fact, given a composition series (M_k) for M, denote $N_k = N \cap M_k$. One has $N_k/N_{k+1} \subset M_k/M_{k+1}$ so each step is simple or zero. Thus, (N_k) will become a composition series for N if one throws out all repetitions. In particular, $l(N) = l(M)$ would mean there are no repetitions, so all $N_k/N_{k+1} \to M_k/M_{k+1}$ are isomorphisms which is only possible when $N_k = M_k$ (induction in k) and, therefore, $N = M$.
- Any chain in M has length $\leq l(M)$. In fact, of (M_k) is a chain of length n, $l(M) = l(M_0) > \ldots > l(M_n) = 0$, that is $l(M) \geq n$. This implies that any composition series has length $l(M)$ as, by definition, $l(M)$ is the minimal length of a composition series.
- Finally, any chain, if it is not a composition series, can be completed, and since the length of a chain is bounded, it can be completed to a composition series.

□

2.5.2. **Proposition.** *M has finite length iff it satisfied both a.c.c. and d.c.c.*

Proof. If M has finite length $l(M)$, any chain has length $\leq l(M)$, so M satisfied both a.c.c. and d.c.c.

Conversely, let M satisfy both chain conditions.Put $M = M_0$ and define M_1 as a maximal submodule different from M_0. Such submodule exists by a.c.c. In the same way one can find M_2 maximal submodule of M_1 et cetera. The sequence $M_0 \supset M_1 \supset \ldots$ stabilizes by d.c.c. This gives a composition series. □

One has

2.5.3. **Theorem.** *(Jordan-Hölder) Let M have length n and let (M_k), (N_k) be its two composition series. Then there exists a permitation $s \in S_n$ such that M_i/M_{i+1} is isomorphic to $N_{s(i)}/N_{s(i)+1}$.*

Proof. The proof will go by induction in n. There is nothing to prove if $n = 1$.

In general, there are two cases: $N_1 = M_1$ and $N_1 \neq M_1$. In the first case we immediately get the result by induction, so we can think $N_1 \neq M_1$.

In this case $N_1 + M_1 = M$ as this is the submodule of M strictly containing M_1. Look at $K = M_1 \cap N_1$. One has $M_1/K \simeq M/N_1$ and $N_1/K \simeq M/M_1$. Choose a composition series for K, $K = K_0 \supset \ldots \supset K_m$, and complete it in two ways to a composition series for M:

$$M \supset M_1 \supset K \supset \ldots$$

and

$$M \supset N_1 \supset K \supset \ldots.$$

They have obviously the same composition factors. But, by inductive hypothesis, the first one has the same factors as

$$M \supset M_1 \supset \ldots \supset M_n,$$

whereas the second has the same factors as

$$M \supset N_1 \supset \ldots \supset N_n.$$

This implies the claim. □

2.6. **Tensor product, I.** We will define now a new operation with modules, their tensor product.

- It is very important in both algebra and geometry.
- It is intimately related to the functor assigning to a pair of modules, M and N, the group of module homomorphisms $\mathrm{Hom}(M, N)$.

We will first study tensor product of vector spaces. Fix a field k.

2.6.1. **Definition.** Let V, W, X be three vector spaces over k. A k-bilinear map $f : V \times W \to X$ is a map satisfying the following properties.

1. $f(v + v', w) = f(v, w) + f(v', w)$.

2. $f(av, w) = af(v, w)$ for any $a \in k$.
3. $f(v, w + w') = f(v, w) + f(v, w')$.
4. $f(v, aw) = af(v, w)$ for any $a \in k$.

Of course, we have already seen this definition in a special case $V = W$ and $X = k$ — this was the definition of a bilinear form on V.

The set of bilinear maps $V \times W \to X$ is a vector space: the sum of two bilinear maps is bilinear and a bilinear map multiplied by a constant is bilinear. We denote $\mathtt{Bil}(V, W; X)$ this vector space.

2.6.2. It is easy to see that $\mathtt{Bil}(V, W; X)$ is a functor in three arguments, covariant in X and contravariant in V and in W. Here is the precise statement.

Given $a : V' \to V$, $b : W' \to W$ and $c : X \to X'$ linear maps, a map

$$\mathtt{Bil}(V, W; X) \to \mathtt{Bil}(V', W', X')$$

is defined as the one carrying $f : V \times W \to X$ to the composition

$$V' \times W' \xrightarrow{a \times b} V \times W \xrightarrow{f} X \xrightarrow{c} X'.$$

Of course, one has to verify that the above composition remains bilinear.

2.6.3. It turns out, for given V and W, there exists a universal bilinear map $u : V \times W \to U$ in the following sense.

As we said above, any linear map $\phi : U \to X$ defines, by composition, a bilinear map $\phi \circ u : V \times W \to X$.

Definition. A bilinear map $u : V \times W \to U$ is called universal if for any vector space X the map

$$\mathrm{Hom}(U, X) \to \mathtt{Bil}(V, W; X)$$

is a bijection (an isomorphism of vector spaces).

The definition above says nothing about existence or uniqueness of the universal bilinear map. We will prove existence later. We will start explaining in what sense it is unique.

2.6.4. **Lemma.** *Let $u : V \times W \to U$ and $u' : V \times W \to U'$ be both universal. Then there exists a unique isomorphism $\theta : U \to U'$ such that $u' = \theta \circ u$.*

Proof. Since u is universal, there exists a unique homomorphism $\theta : U \to U'$ such that $u' = \theta \circ u$. Similarly, since u' is universal, there exists a unique homomorphism $\theta' : U' \to U$ such that $u = \theta' \circ u'$. We claim that θ and θ' are inverse to each other. In fact, $\theta' \circ \theta : U \to U$ satisfies the property

$$u = (\theta' \circ \theta) \circ u$$

and id_U should be the only map $U \to U$ satisfying this property (once more, because of universality of u). The proof of $\theta \circ \theta' = \mathrm{id}_{U'}$ goes along the same lines. □

2.6.5. *Existence.* We will now prove existence of a universal bilinear map. Let X be a basis of V and Y a basis of W. This means that any $v \in V$ can be uniquely presented as a lilnear combination of elements of X, and any element $w \in W$ has a unique presentation of elements of Y. A bilinear map $f : V \times W \to Z$ is uniquely defined by its values on $X \times Y$, $f(x, y) \in Z$. This is the reasoning we know from the theory of bilinear forms.

This leads us to the following construction of a universal bilinear map. Set U to be the vector space with the basis $X \times Y$. We will denote the pair $(x, y) \in X \times Y$ considered as an element of the basis of U, as $x \otimes y$. (At the moment, this is just a notation!)

The map $u : V \times W \to U$ is the one carrying the pair $(x, y) \in V \times W$ to the basis vector $x \otimes y$ of U.

The above description is not easy to understand. To understand it better, let us add that, for $v = \sum c_i x_i$, $w = \sum d_j y_j$, $c_i, d_j \in k$, $x_i \in X$, $y_j \in Y$, one has

$$u(v, w) = \sum_{i,j} c_i d_j x_i \otimes y_j.$$

This easily follows from bilinearity of U and from the condition $u(x_i, y_j) = x_i \otimes y_j$.

2.6.6. We define the tensor product of V and W as "the" universal bilinear map $u : V \times W \to U$. We denote $U = V \otimes W$. This is a vector space, together with a bilinear map $u : V \times W \to U \otimes W$ defined uniquely up to a unique isomorphism.

We also denote $u(v, w)$ as $v \otimes w \in V \otimes W$. This extends the notation $x \otimes y$ we introduced in the construction of $V \otimes W$.

2.6.7. **Corollary.** $\dim(V \otimes W) = \dim(V) \dim(W)$.

□

A bilinear map $f : V \times W \to X$ can be otherwise defined as a linear map $\tilde{f} : V \to \mathrm{Hom}(W, X)$ from V to the vector space $\mathrm{Hom}(W, X)$ of linear maps from W to X. Since one has a bijection $\mathtt{Bil}(V, W; X) = \mathrm{Hom}(V \otimes W, X)$, we get a functorial isomorphism

$$\mathrm{Hom}(V \otimes W, X) \xrightarrow{\sim} \mathrm{Hom}(V, \mathrm{Hom}(W, X)). \tag{16}$$

The above formula connects two functors: tensor product and Hom. In the language of category theory, this means that the functors $\otimes$ and Hom are *adjoint*.

2.6.8. There is another conection between tensor product and the functor Hom. We know that, if V and W have (finite) dimensions m and n respectively, than both $V \otimes W$ and $\mathrm{Hom}(V, W)$ have dimension mn. Here is a more precise connection between the two notions.

For amy pair of vector spaces V and W we define a linear map

$$\theta : V^* \otimes W \to \mathrm{Hom}(V, W)$$

as follows. We start with a bilinear map

$$\Theta : V^* \times W \to \mathrm{Hom}(V, W)$$

by the formula

$$\Theta(f, w)(v) = f(v) \cdot w.$$

Linearity in $f \in V^*$ and in $w \in W$ is obvious. Therefore, by universality of tensor product, we have a linear map θ. We have

Proposition. *Assume that V is finite dimensional. Then θ is an isomorphism.*

Proof. Choose a basis $v_1, \ldots, v_n$ of V. Let $f_1, \ldots, f_n$ be the dual basis for V^*. Recall that this means that $f_j(v_j) = \delta^i_j$, the Kronecker's delta. If $\{w_\alpha\}$ is a basis for W (finite or infinite), the pairs (f_i, w_α) form a basis for $V^* \otimes W$. The map θ carries such pair to the map $\phi_{i,\alpha} : V \to W$ carrying v_i to w_α and v_j for $j \neq i$ to zero. Such $\phi_{i,\alpha}$ form obviously a basis for $\mathrm{Hom}(V, W)$. □

2.6.9. A k-algebra A is a vector space over k with an associative bilinear operation

$$A \times A \to A.$$

Bilinearity is expressed in the distributive properties,

$$(x + y)z = xz + yz, x(y + z) = xy + xz, \tag{17}$$

as well as the properties

$$(ax)y = a(xy),\ x(ay) = a(xy).$$

Thus, we can encode these properties by saying that one has a map $A \otimes A \to A$ satisfying the associativity property.

2.7. **Tensor product, II.** We will now generalize the notion of tensor product to modules over commutative rings.

Note that there is a notion of tensor product for modules over non-commutative rings. We will comment on this notion later, but won't study it in detail.

2.7.1. *Bilinear maps.* We follow the same approach as for the vector spaces – starting with the notion of bilinear map.

Definition. Let M, N, X be three modules over a commutative ring A. An A-bilinear map $f : M \times N \to X$ is a map satisfying the following properties.

1. $f(m + m', n) = f(m, n) + f(m', n)$.
2. $f(am, n) = af(m, n)$ for any $a \in A$.
3. $f(m, n + n') = f(m, n) + f(m, n')$.
4. $f(m, an) = af(m, n)$ for any $a \in A$.

2.7.2. *Universal bilinear map.* Also in this more general context, we define tensor product of M and N (denoted $M \otimes_A N$ or $M \otimes N$ if the basic ring A is clear from the context) as the universal A-bilinear map

$$u : M \times N \to M \otimes N.$$

Precisely as for veector spaces we deduce that, if a universal A-bilinear map exists, it is unique up to unique isomorphism.

It remains to prove existence.

2.7.3. *Construction.* We cannot construct a tensor product of modules by choosing a basis: very few modules have a basis.

This is why our construction will be slightly more sophisticated.

The first step is to define a free module F whose basis is the direct product (of sets) $M \times N$. Let us denote the basis element corresponding to a pair $(m, n) \in M \times N$ by $m * n$. An element of F is a finite linear combination of different $m * n$ with coefficients in A. For any A-module X a homomorphism $f : F \to X$ is uniquely defined by the collection of $f(m * n) \in X$.

We define $\tilde{u} : M \times N \to F$ by the formula $\tilde{u}(m, n) = m * n$. We have a bijection

$$\mathrm{Hom}_A(F, X) = \mathrm{Map}(M \times N, X) \tag{18}$$

between the set of A-linear homomorphisms from F to X and the set of maps $M \times N \to X$, carrying $f \in \mathrm{Hom}_A(F, X)$ to $f \circ \tilde{u}$.

The bijection (18) is slightly similar to what we need, but not precisely. Instead of all maps $M \times N \to X$ in the right-hand side, we want to describe only those that are A-bilinear. Let us repeat what does bilinearity mean. A map $f : M \times N \to X$ is bilinear iff

1. $f(m + m', n) = f(m, n) + f(m', n)$.
2. $f(am, n) = af(m, n)$ for any $a \in A$.
3. $f(m, n + n') = f(m, n) + f(m, n')$.
4. $f(m, an) = af(m, n)$ for any $a \in A$.

We will rewrite these properties once more, using the homomorphism $\tilde{f} : F \to X$ extended by linearity from f. We can rewrite

1. $\tilde{f}((m + m') * n - m * n - m' * n) = 0$.
2. $\tilde{f}((am) * n - a(m * n)) = 0$ for any $a \in A$.
3. $\tilde{f}(m * (n + n') - m * n - m * n') = 0$.
4. $\tilde{f}(m * (an) - a(m * n)) = 0$ for any $a \in A$.

Now we can use the Isomorphism theorem. Define F' as the A-submodule of F generated by all the expressions of the form

$$(m+m')*n-m*n-m'*n,\ (am)*n-a(m*n),\ m*(n+n')-m*n-m*n',\ m*(an)-a(m*n).$$

A homomorphism $\tilde{f} : F \to X$ satisfying the above conditions, is the same as a homomorphism from F/F' to X. Thus, if we denote $M \otimes_A N = F/F'$ and define

$u : M \times N \to M \otimes N$ as the composition of $\tilde{u}$ with the canonical projection, we get the required properties.

2.7.4. *Functoriality of the tensor product.* Here A is a commutative ring. We will write $M \otimes N$ instead of $M \otimes_A N$ for simplicity.

Given a bilinear map $M \times N \to X$ and a homomorphism $M' \to M$, the composition $M' \times N \to M \times N \to X$ is bilinear. This, by universality, defines a homomorphism $M' \otimes N \to M \otimes N$. Thus, tensor product is a functor in the first argument. In the same way it is a functor in the second argument.

2.7.5. *Commutativity.* Let us compare $M \otimes N$ with $N \otimes M$. One has two universal bilinear maps:

$$u_{M,N} : M \times N \to M \otimes M$$

and

$$u_{N,M} : N \times M \to N \otimes M.$$

We also have an obvious map $s : M \times N \to N \times M$ carrying (m, n) to (n, m). The map s is a bijection and so both $u_{M,N}$ and $u_{N,M} \circ s$ are universal bilinear maps.

This has to be verified; the verification is immediate and is left to reader.

This implies that there is a unique isomorphism $\theta : M \otimes N \to N \otimes N$ such that

$$\theta \circ u_{M,N} = u_{N,M} \circ s.$$

the last equality can be rewritten as

$$\theta(m \otimes n) = n \otimes m.$$

2.7.6. *Associativity.* We can consider trilinear maps $M \times N \times K \to X$ and look for a universal such map. As usual, it is unique up to unique isomorphism, if it exists. Now, it is easy to present two such universal maps:

- $M \times N \times K \to (M \otimes N) \otimes K$ defined as the composition

  $$M \times N \times K \xrightarrow{s} (M \times N) \times K \to (M \otimes N) \times K \to (M \otimes N) \otimes K,$$

- $M \times N \times K \to M \otimes (N \otimes K)$ defined as the composition

  $$M \times N \times K \xrightarrow{s} M \times (N \times K) \to M \times (N \otimes K) \to M \otimes (N \otimes K).$$

Also here the trilinearity and the universality has to be verified.

This gives a unique isomorphism

$$(M \otimes N) \otimes K \to M \otimes (N \otimes K).$$

This is the correct formulation of associativity property of tensor product.

2.7.7. *Adjunction.* Similarly to the case of vector spaces, see isomorphism (16), we have an isomorphism of functors

$$\mathrm{Hom}_A(M \otimes N, X) \xrightarrow{\sim} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, X)). \tag{19}$$

This immediately follows from the fact that a bilinear map $f : M \times N \to X$ can be equivalently described a homomorphism from M to $\mathrm{Hom}_A(N, X)$.

2.7.8. *Distributivity.* We will prove that there is a natural isomorphism

$$\sum_{i \in I} M_i \otimes N = \sum_{i \in I} (M_i \otimes N).$$

We will denote by L the left-hand side of the formula and by R the right-hand side of the formula. Let X be an arbitrary A module and let us describe $\mathrm{Hom}_A(R, X)$. We have

$$\mathrm{Hom}_A(R, X) = \prod_{i \in I} \mathrm{Hom}_A(M_i \otimes N, X)$$

as $\mathrm{Hom}_A(\_, X)$ carries direct sums to direct products. On the other hand,

$$\mathrm{Hom}_A(L, X) = \mathrm{Hom}_A(\sum_{i \in I} M_i, \mathrm{Hom}_A(N, X)) = \prod_{i \in I} \mathrm{Hom}_A(M_i, \mathrm{Hom}_A(N, X)) = \prod_{i \in I} \mathrm{Hom}_A(M_i \otimes N, X).$$

we get the same formula, so L and R should be isomorphic.

We will explain the last point giving a precise general (category theory) argument.

2.7.9. **Lemma.** *Assume we have an isomorphism*

$$\theta_X : \mathrm{Hom}(L, X) \to \mathrm{Hom}(R, X)$$

functorial in X. Then there is a unique isomorphism $t : R \to L$ such that θ_X carries $f : L \to X$ to the composition $f \circ t$.

Proof. We put $t = \theta_L(\mathrm{id}_L)$. This is an isomorphism as its inverse is $\theta_R^{-1}(\mathrm{id}_R)$. It remains to verify that the isomorphism t satisfies the required property $\theta_X(f) = f \circ t$. This follows from functoriality of θ leading to the following commutative diagram.

$$\begin{array}{ccc} \mathrm{Hom}(L, L) & \xrightarrow{\theta_L} & \mathrm{Hom}(R, L) \\ \downarrow f & & \downarrow f \\ \mathrm{Hom}(L, X) & \xrightarrow{\theta_X} & \mathrm{Hom}(R, X) \end{array} \tag{20}$$

The diagram implies the formula $\theta_X(f) = f \circ \theta_L(\mathrm{id}_L)$ □

2.7.10. *Right exactness.* We remember that the functor Hom is left exact. We will now prove that the tensor product functor is right exact. To do so, we will prove a converse to 1.7.4:

Lemma. *Let*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{21}$$

be a complex, so that for any module P the complex

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

is exact. Then the original complex is exact.

Proof. Put $P = M''/\operatorname{Im}(g)$. The natural projection $M'' \to P$ goes to zero, so $P = 0$ that is g is surjective. Now put $P = M/\operatorname{Im}(f)$ and let $p : M \to P$ be the natural projection. By the conditions of the lemma, p factors through g which implies that $\operatorname{Ker}(g) \subseteq \operatorname{Ker}(p) = \operatorname{Im}(f)$. □

Now are now ready to prove the following.

Proposition. *Let (21) be exact. Then for any A-module N the sequence*

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

is also exact.

Proof. According to the above lemma, it is sufficient to prove that, for any P the sequence

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

is exact. Using the adjunction isomorphism, we can rewrite this sequence as

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

which is exact by left exactness of the functor Hom. □

2.7.11. *Examples.* Tensor product of free modules look similar to tensor product of vector spaces:

$$F(X) \otimes F(Y) = F(X \times Y).$$

Let us think about $\otimes_{\mathbb{Z}}$.

I claim that for any abelian group G one has an isomorphism

$$\mathbb{Z}_n \otimes G \to G/nG.$$

By definition, this tensor product is a universal bilinear map $f : \mathbb{Z}_n \times G \to X$. A bilinear map $f : \mathbb{Z}_n \times G \to X$ is uniquely given by a group homomorphism $\phi : G \to X$ where $\phi(g) = f(1, g)$. This is because by bilinearity $f(r, g) = rf(1, g) = r\phi(g)$. However, not every homomorphism ϕ defines a bilinear map f.

One should have $\phi(ng) = n\phi(g) = f(n, g) = 0$. Thus, bilinear map $\mathbb{Z}_n \times G \to X$ are uniquely described by the homomorphisms $\phi : G \to X$ satisfying the condition $\phi(ng) = 0$. In other words, they are uniquely described by homomorphisms $G/nG \to X$. This actually proves that the univervsal bilinear map is given by $f : \mathbb{Z}_n \times G \to G/nG$ defined by the formula $f(r, g) = rg + nG$.

2.8. **Flat modules.**

2.8.1. **Definition.** A module M is called flat if the functor $\_ \otimes_A M$ is exact.

One has the following equivalent characterization of flat modules.

2.8.2. **Proposition.** *The following conditions for an A-module M are equivalent.*

1. *M is flat.*
2. *For any injective map $N' \to N$ the induced map $N' \otimes_A M \to N \otimes_A M$ is injective.*
3. *For any ideal $I \subset A$ the map $I \otimes_A M \to A \otimes_A M = M$ is injective.*
4. *For any injective module J the module $\mathrm{Hom}_A(M, J)$ is injective.*

Proof. The tensor product is right exact, so the conditions 1 and 2 are equivalent. Furthermore, Condition 2 trivially implies condition 3.

Let us show that 3 implies 4. To verify injectivity of $\mathrm{Hom}_A(M, J)$, it is enough to prove that for any ideal I in A the restriction map

$$\mathrm{Hom}_A(A, \mathrm{Hom}_A(M, J)) \to \mathrm{Hom}_A(I, \mathrm{Hom}_A(M, J))$$

is surjective. By adjointness, this is equivalent to the surjectivity of

$$\mathrm{Hom}_A(A \otimes_A M, J) \to \mathrm{Hom}_A(I \otimes_A M, J).$$

This condition holds since J is injective and M satisfies Condition 3.

Let us now deduce Condition 2 from 4. Let K be the kernel of the map $N' \otimes_A M \to N \otimes_A M$.

Let J be any injective module. The sequence

$$\mathrm{Hom}_A(N \otimes_A M, J) \xrightarrow{\phi} \mathrm{Hom}_A(N' \otimes_A M, J) \to \mathrm{Hom}_A(K, J) \to 0$$

is exact. The map ϕ is surjective as, by Condition 4, the module $\mathrm{Hom}_A(M, J)$ is injective. Therefore, $\mathrm{Hom}_A(K, J) = 0$ for any injective J. This is only possible if $K = 0$ as otherwise K can be embedded into an injective and this embedding yields a nonzero map. □

2.9. **Variants.** Assume now that A is not necessarily commutative. It turns out that we still can define A-bilinear maps.

2.9.1. **Definition.** Let M be a right A-module, N a left A-module, X an abelian group. A map

$$f : M \times N \to X$$

is called A-bilinear if the following conditions are fulfilled.

1. $f(m+m',n) = f(m,n) + f(m',n)$.
2. $f(m,n+n') = f(m,n) + f(m,n')$.
3. $f(ma,n) = f(m,an)$.

Similarly to the commutative case, we define tensor product as a universal A-bilinear map $u : M \times N \to M \otimes_A N$.

Thus, tensor product of a right A-module with a left A-module gives an abelian group.

One can get more if M or N (or both) has an extra structure.

2.9.2. **Definition.** Let A and B be two rings. An (A,B)-bimodule is a left A-module M having a structure of a ring B-modules, such that

$$(am)b = a(mb).$$

Given three rings A, B, C, an (A,B)-bimodule M and a (B,C)-bimodule N, the tensor product $M \otimes_B N$ has a structure of (A,C)-bimodule, so that $a(m \otimes n)c = am \otimes nc$.

Here is how to verify this. We have a universal B-linear map $M \times N \to M \otimes_B N$. Given $a \in A$, we have a composition

$$M \times N \to M \times N \xrightarrow{u} M \otimes_B N,$$

with the first map carrying (m,n) to (am,n). By universality of u, it defines a unique map $M \otimes N \to M \otimes N$ which is action of $a \in A$ on the left. The right C-module structure is defined similarly.

One has to verify that these two module structures are compatible

Many properties of tensor product over a commutative ring (except for commutativity) have a non-commutative analog.

2.9.3. *Base change.* Given a homomorphism of rings $f : A \to B$ and a left B-module X, we define $f^*(X)$ as the same module, considered as A module via the formula $a \cdot x = f(a)x$.

Similarly, B acquires a structure of (B,A)-bimodule defined by the formula $b' \cdot b = b'b,\ b \cdot a = bf(a)$.

If N is a left A-module, $B \otimes_A N$ becomes a left B-module. the tensor product $B \otimes_A N$ has a structure of B-module, and A-module structure on X is defined by

2.9.4. **Proposition.** *One has a natural isomorphism*

$$\mathrm{Hom}_B(B \otimes_A N, X) = \mathrm{Hom}_A(N, f^*(X)).$$

Proof. By definition, homomorphisms of abelian groups $B \otimes_A N \to X$ are in one-to-one correspondence with A-bilinear maps $B \times N \to X$. This correspondence assigns to $F : B \otimes_A N \to X$ its composition f with the map $B \times N \to B \otimes_A N$ carrying (b,n) to $b \otimes n$.

The elements $b \otimes n$ generate $B \otimes_A N$ as an abelian group. Therefore, they generate it as well as a B-module. So, $F : B \otimes_A N \to X$ is B-linear iff for any $b' \in B$ and $(b, n) \in B \times N$ one has

$$F(b'b \otimes n) = F(b'(b \otimes n)) = b'F(b \otimes n),$$

that is

$$f(b'b, n) = b'f(b, n). \tag{22}$$

It remains to describe A-bilinear maps $f : B \times N \to X$ satisfying the property (22). Any such map carry (b, n) to $gf(1, n)$. Denote $\phi : N \to X$, $\phi(n) = f(1, n)$. The map $f(b, n) = b\phi(n)$ is A-bilinear iff ϕ is A-linear. This yields the required claim. □

Sometimes people allow themselves to write X instead of $f^*(X)$.

The functor $N \mapsto B \otimes_A N$ is called *base change*. The proposition means that base change is left ajoint to f^*.

2.9.5. *Adjoint functors, in general.* Here is a general definition. Given two categories, $\mathcal{C}$ and $\mathcal{D}$, and a pair of functors

$$F : \mathcal{C} \to \mathcal{D},\ G : \mathcal{D} \to \mathcal{D},$$

an adjunction between F and G is a functorial isomorphism

$$\mathrm{Hom}_{\mathcal{D}}(F(x), y) \overset{\text{iso}}{\to} \mathrm{Hom}_{\mathcal{C}}(x, G(y)).$$

Note that F and G have different roles in the definition. F is called left adjoint to G, and G is called a right adjoint to F.

Here are examples of adjoint pairs of functors.

- The functor $F : \mathtt{Set} \to \mathtt{Ab}$ of free abelian group is left adjoint to the forgetful functor $G : \mathtt{Ab} \to \mathtt{Set}$ carrying each abelian group to the underlying set.
- For a commutative ring A and an A-module N, the functor $\otimes_A N$ is left adjoint to $\mathrm{Hom}_A(N, \_)$.
- For a homomorphism of rings $A \to B$, the functor $B \otimes_A \_$ from left A-modules to left B-modules, is left adjoint to the forgetful functor in the opposite directions.

3. Representations of finite groups

We will now apply some of the algebraic ideas we studied to studying group prepresentations.

3.1. **Basic definitions and basic examples.** Let G be a finite group and V a vector space over a fixed field k.

3.1.1. **Definition.** A representation of G in V is a group homomorphism $\rho : G \to GL(V)$.

In other words, a representation ρ assigns to each $g \in G$ a linear operator $\rho(g) : V \to V$, so that $\rho(g)\rho(h) = \rho(gh)$.

If we choose a basis in V, the elements $\rho(g)$ are presented by matrices, so we have got a presentation of elements of G by matrices. This explains the terminology.

Recall that a group G defines a k-algebra $kG = \oplus_{g\in G} k \cdot g$ (group algebra) with the multiplication defined by the multiplication in G. Here is an equivalent definition of representation.

3.1.2. **Definition.** A representation of G is just a kG-module.

Thus, we do not have to repeat the notions of subrepresentation (=submodule), direct sum of representations, irrreducible representation (=simple module).

Here is a first remarkably easy fact.

3.1.3. **Theorem.** *Assume* $\mathrm{char}(k)$ *and* $|G|$ *are coprime (no condition if* $\mathrm{char}(k) = 0$*). Then the group algebra* kG *is semisimple.*

Proof. The condition on $\mathrm{char}(k)$ is equivalent to saying that $|G|$ is invertible in k. Recall that a ring is semisimple if the category of left modules is semisimple, that is, if any epimorphism $f : M \to N$ splits. Let $g : N \to M$ be a linear transformation splitting f. We will "correct" g so that the result $\tilde{g}$ will be a morphism of representations, and it will still split f.

We define $\tilde{g} : N \to M$ by the following formula.

$$\tilde{g}(n) = \frac{1}{|G|} \sum_{x\in G} x(g(x^{-1}(n))).$$

Let us verify the conditions. First of all, let us verify that $\tilde{g}$ is a map of representations. This means that, for any $n \in N$ and $y \in G$ we should verify that $\tilde{g}(yn) = y\tilde{g}(n)$. We have

$$|G|\tilde{g}(yn) = \sum_{x\in G} x(g(x^{-1}(yn))) = y \sum_{x\in G} y^{-1}x(g(x^{-1}(yn))) = y \cdot |G|\tilde{g}(n). \tag{23}$$

It remains to verify that $\tilde{g}$ splits f. We have

$$f(\tilde{g}(n)) = \frac{1}{|G|} \sum_{x\in G} f(x(g(x^{-1}(n)))) = \frac{1}{|G|} \sum_{x\in G} n = n. \tag{24}$$

□

We can say even more if k is algebraically closed.

3.1.4. **Lemma.** *(Schur lemma) Let k be algebraically closed and V be an irreducible representation of G. Then any G-endomorphism of V is a multiplication by $c \in k$.*

Proof. We proved a form of Schur lemma saying that endomorphisms of V form a division algebra. We now prove a stronger claim.

First of all, any irreducible represntation is finite-dimensional — this immediately follows from the fact that $\dim(kG) = |G| < \infty$. Let $f : V \to V$ be a G-endomorphism. Since k is algebraically closed, f gas an eigenvalue $\lambda \in K$. Then $f - \lambda \cdot \mathrm{id}$ is not invertible, therefore, is zero. □

3.1.5. **Corollary.** *Let k be algebraically closed and let $V_1, \dots, V_m$ be (representatives of) all irreducible representations of G. Then kG is isomorphic to a product of matrix rings over k.*

3.1.6. *One-dimensional representations.* For any group G one-dimensional vector space k with the trivial action, $g(x) = x$, is a representation called *the trivial representation*.

Let us describe all one-dimensional representations. These are group homomorphisms $\chi : G \to k^*$.

For any $g, h \in G$ one has $\chi(ghg^{-1}h^{-1}) = 1$ as k^* is commutative. So χ is trivial on the commutator subgroup $[G, G]$ of G. Thus, description of one-dimensional representations reduces to description of homomorphisms of abelian groups $G^{ab} := G/[G, G] \to k^*$.

In the case when G is finite, G^{ab} is also finite, so is isomorphic to a direct sum of cyclic groups. A homomorphism from a cyclic group $\mathbb{Z}_n$ to k^* is given by an n-th root of unity in k.

This solves the problem.

Group homomorphisms $\chi : G \to \mathbb{C}^*$ are called *multilicative characters* of G.

The trivial character $\chi = 1$ corresponds to the trivial representation.

Exercises: Describe all multilicative characters of $\mathbb{Z}_n$. Prove that an abelian group of order n has n different multiplicative characters.

3.1.7. *The case G is commutative.* We claim

Proposition. *Any irreducible representation of a finite commutative group G over an algebraically closed field is one-dimensional.*

Proof. Any irreducible representation is finite dimensional. We will now prove that such representation V has a vector v which is common eigenvector for all $g \in G$. We do the following. Choose an eigenvector $v \in V$ for some $g \in G$. Assume $\lambda \in k^*$ is the respective eigenvalue. Let $V' = \{x \in V | g(x) = \lambda x\}$. By Lemma below V' is a subrepresentation of G. Since V is irreducible, $V' = V$, so g acts on V as multiplication by λ. □

3.1.8. **Lemma.** *Let f, g be two commuting operator on a vector space V. Let $\lambda \in k$ and $V' = \{x \in V | g(x) = \lambda x\}$. Then V' is an invariant subspace with respect to f.*

Proof. If $x \in V'$, $g(f(x)) = f(g(x)) = f(\lambda x) = \lambda f(x)$. This implies that $f(x) \in V'$ as required. □

3.1.9. *More examples.* Let X be a set and let G act on X. Denote $V = kX$ the vector space generated by X (X is a basis of V). Then a prepresentation of G in V is defined. for instance, the group S_n acts on the set $\{1, \dots, n\}$ in a natural way. This defines an n-dimensional representation of S_n.

Exercise: prove this representation is not irreducible (Hint: it has a trivial subrepresentation).

3.2. **Operations with representations.** Given two vector spaces V and W, we can define $\mathrm{Hom}(V, W)$ and $V \otimes W$. If V and W are representations of G, there is a natural structure of G module on $\mathrm{Hom}(V, W)$ and $V \otimes W$.

3.2.1. **Remark.** The tensor product and the Hom considered here are not over kG: they are tensor product and Hom of vector spaces!

3.2.2. Hom. Let V and W be representations of G. For $f : V \to W$ we define $g(f) : V \to W$ by the formula $g(f)(v) = g(f(g^{-1}v))$. Things to verify:

- That $g(f)$ so defined is linear.
- That g so defined is linear, that is that $g(av + bv') = ag(v) + bg(v')$.
- That $g(h(v)) = (gh)(v)$.

All verifications are routine.

3.2.3. *Dual representation.* In particular, take $W = k$ — the trivial representation. We get the representation of G on $V^* = \mathrm{Hom}(V, k)$. It is given by the formula

$$g(f)(v) = f(g^{-1}(v)).$$

The vector space V^* with the defined above structure of G-module is called *the dual representation.*

3.2.4. *Another* Hom. We have just defined a representation $\mathrm{Hom}(V, W)$ whose underlying vector space is the space of all linear maps from V to W.

There is another one, the vector space of all kG-homomorphism from V to W. We will denote it by $\mathrm{Hom}_G(V, W)$.

By definition, $\mathrm{Hom}_(V, W) \subset \mathrm{Hom}(V, W)$. Since $G \subset kG$ generates the whole ring,

$$\mathrm{Hom}_G(V, W) = \{f : V \to W | \forall (g \in G) f(g(v)) = g(f(v))\}.$$

Taking into account the G-module structure on $\mathrm{Hom}(V, W)$, we get the following.

Proposition. $\mathrm{Hom}_G(V, W) = \{f \in \mathrm{Hom}(V, W) | \forall (g \in G) g(f) = f\}$.

3.2.5. *Tensor product.* Given V and W as above, we will define a representation of G in the vector space $V \otimes W$. For any $g \in G$ we have to define $g : V \otimes W \to V \otimes W$. This is done by functoriality: the maps $g_V : V \to V$ and $g_W : W \to W$ define $g := g_V \otimes g_W : V \otimes W \to V \otimes W$. All verifications are obvious.

The following formula defines the actiuniquely determines the G-module structure on $V \otimes W$.

$$g(v \otimes w) = g(v) \otimes g(w).$$

3.2.6. *Properties.* One has the adjunction isomorphism of vector spaces.

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

If V, W and U are representations of G, we have the structures of G-module on the left and on the right-hand side. We claim that the above isomorphism is compatible with these structures.

This is an easy exercise.

Here is another compatibility. We know that, if W is finite dimensional, the map

$$V^* \otimes W \to \mathrm{Hom}(V, W)$$

is an isomorphism. We claim that this isomorphism is also an isomorphism of G-modules, once V and W have G-module structures.

3.3. **Characters.** Group homomorphisms $\chi : G \to \mathbb{C}^*$ classify one-dimensional representations. We called them *multiplicative characters.* We will now assign to each finite dimensional representation V of a group G a map $\chi_V : G \to \mathbb{C}$ called *a character of* V. This will be a generalization of the notion of multiplicative character. We will see that characters contain a lot of information about representation, so that one can reduce a study of representations to studying characters.

3.3.1. **Definition.** Given a complex finite dimensional representation V of G, we define $\chi_V : G \to \mathbb{C}$ by the formula

$$\chi_V(g) = \mathrm{tr}\{g : V \to V\}.$$

In the case $\dim V = 1$ the character of V is precisely the group homomorphism $\chi : V \to \mathbb{C}^*$ we met before.

3.3.2. **Proposition.** *Let V be a complex representation of dimension n, $\chi = \chi_V$.*

1. $\chi(1) = n$.
2. $\chi(g^{-1}) = \overline{\chi(g)}$.
3. $\chi(hgh^{-1}) = \chi(g)$.

Proof. Note that g has finite order, so all its eigenvalues are roots of unity, so satisfy the property $\lambda^{-1} = \overline{\lambda}$. The element g^{-1} has the eigenvalues inverse to that for g. This implies Claim 2. □

A function $\chi : G \to \mathbb{C}$ is called *a class function.* The proposition above says that any character is a class function.

3.3.3. *Regular representation.* Look at $\mathbb{C}G$ as a module over itself. It gives a representation of dimension $n = |G|$ called *the regular representation.* Let us calculate its character.

We have

Lemma. *The character χ^{reg} of the regular representation takes value n at 1 and 0 otherwise.*

Proof. For $g \neq 1$ the matrix of g in the standard basis has no nonzero entries in the diagonal. □

It is ineresting to see what happens to the characters under different operations with represenations.

3.3.4. **Proposition.**
1. $\chi_{V\oplus W} = \chi_V + \chi_W$.
2. $\chi_{V\otimes W} = \chi_V \cdot \chi_W$.
3. $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V} \cdot \chi_W$.

Proof. The following idea simplifies the reasoning. We have to compare two functions on G. To do so, we are allowed, for any $g \in G$, to choose a basis for all representations so that g will be presented by a diagonal matrix.

1. This claim is obvious.

2. Choose bases $v_1, \dots, v_n$ in V and $w_1, \dots, w_m$ for W so that g is diagonal: $g(v_i) = a_i v_i,\ g(w_j) = b_j w_j$. Then the collection $v_i \otimes w_j$ fors a basis for $V \otimes W$, g is diagonal in this basis with the eigenvalues $a_i b_j$. Their sum is $(\sum a_i)(\sum b_j)$.

3. With the same bases for V and W, $\mathrm{Hom}(V, W) = V^* \otimes W$ has basis $\{v_i^* \otimes w_j\}$. It remains to add that if $g(v_i) = a_i v_i$ then $g(v_i^*) = \overline{a_i} v_i^*$. □

3.3.5. We will now determine,in terms of the character, the dimension of the invariant subspace of a representation V.

For a representation V we denote

$$V^G = \{x \in V | \forall g \in G\ g(v) = v\}.$$

The following observation is very important.

Lemma. *The linear operator*

$$\rho : V \to V,\ \rho(v) = \frac{1}{|G|} \sum_{g\in G} g(v)$$

is a projection of V to V^G.

Proof. The lemma claims that $\rho(V) \subset V^G$ and that $\rho|_{V^G} = \mathrm{id}$. Let us first verify the second claim. If $v \in V^G$, $\rho(v) = \frac{1}{|G|}\sum_{g\in G} v = v$. For the first claim,

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

□

Corollary. *One has* $\dim V^G = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)$.

Proof. This is because $\dim V^G = \mathrm{tr}(\rho)$. □

3.4. **Inner product.** Given $\phi, \psi : G \to \mathbb{C}$ we define their inner product by the formula

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

We have the following result.

3.4.1. **Theorem.** 1. *Let V, W be two representations. Then*

$$\dim \mathrm{Hom}_G(V, W) = (\chi_V|\chi_W).$$

2. *Characters of irreducible prepresentations have length one; different irreducible representations are orthogonal.*

Proof. We know that $\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G$, so

$$\dim \mathrm{Hom}_G(V, W) = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_W(g) = (\chi_V|\chi_W).$$

The second claim follows from Schur lemma. □

We will now prove that the characters of the irreducible representations form an orthonormal basis in the space of class functions.

The characters of irreducible representations are called *the irreducible characters.*

3.4.2. **Theorem.** *Let $f : G \to \mathbb{C}$ be a central function orthogonal to all irreducible characters. Then $f = 0$.*

Proof. Define an element $\rho_f \in \mathbb{C}G$ by the formula

$$\rho_f = \frac{1}{|G|}\sum_{g\in G} f(g)g.$$

The element ρ_f defines, for any representation V, an endomorphism $\rho_f : V \to V$ carrying $v \in V$ to $\frac{1}{|G|}\sum_{g\in G} f(g)g(v)$. Since f is a class function, ρ_f is an endomorphism of $\mathbb{C}G$-modules, that is, that for any $h \in G$ one has $h\rho_f = \rho_f h$.

Therefore, for any irreducible representation V the endomorphism ρ_f^V of V guven by ρ_f, acts as multiplication by a constant, call it c_V. Let us calculate it, in terms of χ_V.

We have $\mathrm{tr}(\rho_f^V) = c_V \cdot \dim(V) = \frac{1}{|G|}\sum_{g\in G} f(g)\chi_V(g) = (\overline{f}|\chi_V)$. Therefore,

$$c_V = \frac{1}{\dim(V)}(\overline{f}|\chi_V).$$

We deduce that if f is orthogonal to all irreducible characters, $\rho_{\overline{f}}$ acts trivially on all irreducible modules. Therefore, it acts trivially on all modules, in particular, on the regular representation. Recall that the regular representation has a basis $\{v_g\}, g \in G$ with the action $h(v_g) = v_{hg}$. By definition, $\rho_{\overline{f}}(v_1) = \frac{1}{|G|}\sum_{g\in G}\overline{f(g)}v_g$. So, $\rho_{\overline{f}}(v_1) = 0$ implies $f(g) = 0$ for all g. □

3.4.3. **Corollary.** *The characters of irreducible representations of G form an orthonormal basis of the space of all class functions on G.*

Proof. The space of class functions has the inner product defined as the restriction of the inner product defined in the beginning of this subsection. The characters of irreducible prepresentations are orthonormal. They generate a subspace whose orthogonal complement is zero by the previous theorem. □

3.5. **Consequences.** Character theory gives a bunch of immediate consequences.

3.5.1. **Corollary.** *The number of irreducible represenntations of a finite group G coincides with the number of conjugacy classes of G.*

3.5.2. **Corollary.** *Let V be an irreducible representation of G of dimension d. Denote by R the regular representation. The representation V appears precisely d times in the decomposition of R into a sum of irreducible representations.*

Proof. The number of copies of V in the decomposition of R is $\dim \mathrm{Hom}_G(V, R) = (\chi_V|\chi_R)$. Since $\chi_R(1) = |G|$ and $\chi_R(g) = 0$ for $g \neq 1$,

$$(\chi_V|\chi_R) = \frac{1}{|G|}|G|\chi_V(1) = d.$$

□

3.5.3. **Corollary.** *Let $V_1, \ldots, V_k$ be all irreducible representations of G and let $\dim(V_i) = d_i$. Then*

$$|G| = \sum_{i=1}^{k} d_i^2.$$

Proof. Immediately follows from the decomposition

$$R = \oplus_{i=1}^{k} V_i^{d_i}.$$

□

3.5.4. *Product of groups.* We will now study representations of a product $G \times H$ of groups. First of all, any representation V of G can be considered to by a representation of $G \times H$, so that $(g, h) \in G \times H$ acts on V like g.

Given V, a representation of G, and W, a representation of H, one defines $V \boxtimes W$, a representation of $G \times H$, as the tensor product of V and W, both considered as representations of $G \times H$. It is easy to prove the following result.

3.5.5. **Theorem.** *The tensor products $V \boxtimes W$, where V is an irreducible representation of G and W is an irreducible representation of W describe all irreducible representations of $G \times H$.*

Proof. First of all, the conjugacy classes of $G \times H$ are in one-to-one correspondence with the pairs of conjugacy classes of G and of H. We will calculate the characters of $V \boxtimes W$ where V and W are irreducible, and show the orthonormality. This will give the result.

First of all, we claim that $\chi_{V \boxtimes W}(g, h) = \chi_V(g) \cdot \chi_W(h)$. This immediately follows from the character formula for the tensor product of representations. This allows one to calculate the inner product

$$(\chi_{V \boxtimes W} | \chi_{V' \boxtimes W'}) = (\chi_V | \chi_{V'})(\chi_W | \chi_{W'}).$$

This implies that the length of $\chi_{V \boxtimes W}$ is one, and that different $V \boxtimes W$ are orthogonal. □

3.6. **Examples.**

3.6.1. $G = \mathbb{Z}/n\mathbb{Z}$. This is an abelian group so all its irreducible representations are one-dimensional. It is instructive to write down explicit formulas for the characters of all irreducible representations and to write down the orthogonality formulas for them. We leave this as an exercise. These formulas look very similar to the formulas for Fourier series and Fourier transform. In fact, this is what is called discrete Fourier transform (see Wikipedia).

3.6.2. $G = S_3$. The group G has three conjugacy classes, and, correspondingly, three irreducible representations. There are two one-dimensional representations (which one?), so the the formula $6 = 1^2 + 1^2 + d^2$ we deduce $d = 2$. That is, apart of the one-dimensional representations, there is a two-dimenaional irreducible representation. The group $G = S_3$ has a standard 3-dimensional representation $V = \mathbb{C}^3$ whose coordinates are permuted by G. The vector $(1, 1, 1)$ spans a trivial representation, so V is a sum of the trivial representation and an irreducible representation of dimension 2. See the Exercise.

3.6.3. *Dihedral group D_8.* It is easy to see that in this case $G^{ab} = \mathbb{Z}_2 \times \mathbb{Z}_2$, so there are four one-dimensional representations. Since $8 - 4 = 2^2$, this leaves only one irreducible 2-dimensional representation.

It is easy to see that the natural representation of D_8 on $\mathbb{R}^2$ gives an irreducible 2-dimensional complex representation. So, all representations are described.

3.6.4. *Real representations.* Our main results were formulated for complex representations. Given a real representation V of a group G, one can define its "complexification" as $V_{\mathbb{C}} := \mathbb{C} \otimes_{\mathbb{R}} V$.

If V is reducible, $V_{\mathbb{C}}$ is also reducible. But the converse does not always hold.

Here is an easy example one should have in mind.

Let $G = \mathbb{Z}_n$. The group G acts on $\mathbb{R}^2$ by rotations: the standard generator rotates $\mathbb{R}^2$ by $\frac{2\pi}{n}$. This is obviously an irreducible representation. As we know, there are no 2-dimensional irreducible representations of $\mathbb{Z}_n$ over $\mathbb{C}$. Exercise: describe the decomposition of the complexification of the 2- dimensional real representation described above.

4. Commutative algebra, 1

We start studying commutative rings. First of all, we need a motivation.

4.1. **Systems of algebraic equations.** Let k be a field, $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ polynomials of n variables.

It is a classical question to find all solutions of the system of polynomial equations

$$f_1(x_1, \dots x_n) = \dots = f_m(x_1, \dots x_n) = 0.$$

4.1.1. We know what to do if $n = 1$. Any collection of polynomials geerate an ideal which is generated by one element. So, a system of polynomial equations is equivalent to a single equation $f = 0$. A solution of this equation in k is equivalent to a ring homomorphism $k[x]/(f) \to k$. Even if there are no solutions in k, it makes sense to look for solutions in a field K containing k. To get all solutions, we have to present f as a product of irreducible polynomials p_i. Each one of them defines a field extension $K = k[x]/(p_i)$, and one has a tautological solution $x + (p_i) \in K$ of the equation.

4.1.2. *Some motivational questions.* The example of $n = 1$ immediately tells us what can be expected in general. The first step is to replace the system of equations $f_i = 0$ with an ideal $I = (f_1, f_2, \dots)$ in the polynomial ring.

One can ask: is I always principal? Well, obviously, no. However, I is finitely generated — this is a famous Hilbert basis theorem. We will prove it soon.

A next question. Let $A = k[x_1, \dots, x_n]/I$. Let K be a field extension of k. A collection of solution $(X_1, \dots, X_n) \in K^n$ of the system of equations $f(X_1, \dots, X_n) = 0,\ f \in I$ is given by ring homomorphisms $\phi : A \to K$. What ideal can appear as a kernel of such homomorphism?

The answer is easy: these are prime ideals (see definition below). Thus, study of prime ideals can be seen as a very general approach to studying solutions of systems of polynomial equations.

4.2. **Prime ideals and maximal ideals.** Let A be a commutative ring.

4.2.1. **Definition.** An ideal $\mathfrak{p} \subset A$, $\mathfrak{p} \neq A$, is called prime if the following equivalent conditions are satisfied.

- for $a, b \in A$ $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- The quotient $A/\mathfrak{p}$ is an integral domain.

In particular, if A is a PID, the ideal (a) is prime iff a is a prime element.

It is clear that for any ring homomorphism $\phi : A \to K$ to a field the kernel $\mathrm{Ker}(\phi)$ is prime: the qutient $A/\mathrm{Ker}(\phi)$ is isomorphic to a subring of K which has no zero divisors.

We will now show that the converse holds.

4.2.2. *Field of fractions.* Given an integral domain A, we will define an injective homomorphism $\phi : A \to K$ into a field.

This will show that any prime ideal $\mathfrak{p}$ of A can be kernel of a homomorphism to a field: it is enough to embed the integral domain $A/\mathfrak{p}$ into a field K and define ϕ as the composition $A \to A/\mathfrak{p} \to K$.

Given an integral domain A, we define its fraction field K as follows. First of all, then X be the set of pairs (a, b) with $a, b \in A$ and $b \neq 0$. We define an equivalence relation on X:

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b.$$

(We will have to use the fact that A is integral domain to verify that this is an equivalence relation.)

We define $K = X/\sim$. We denote the equivalence class of (a, b) as $\frac{a}{b}$.

The operations are defined as the usual operations with fractions:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \ \frac{a}{b}\frac{a'}{b'} = \frac{aa'}{bb'}.$$

4.2.3. As a result, studying of prime ideals in a commutative ring A is a problem very close to studying ring homomorphisms $A \to K$ to fields.

Any prime ideal $\mathfrak{p} \subset A$ defines the integral domain $A/\mathfrak{p}$ which canonically embeds into its field of fraction which we will denote $k(\mathfrak{p})$. Thus, any ring homomorphism $\phi : A \to K$ with $\mathfrak{p} = \mathrm{Ker}(\phi)$ can be canonically decomposed as $A \to k(\mathfrak{p}) \to K$.

4.2.4. Assume A is a PID. Any ideal in A has form (a) where $a \in A$. It is prime iff a is either 0 or a prime (=irreducible) element. Thus, we have the following prime ideals in A:

- (0)
- (p) where p is a prime element of A.

(0) is the minimal ideal and all (p) are the maximal ideals of A.

4.2.5. *Maximal ideals.* Recall that $\mathfrak{m} \subset A$ is called a maximal ideal if $\mathfrak{m}$ is maximal among those $\neq A$. Equivalently, $\mathfrak{m}$ is maximal iff $A/\mathfrak{m}$ is a field. This is because for any ideal I in A there is a one-to-one correspondence between the ideals of A/I and the ideals of A containing I. (Describe this correspondence explicitly!).

In particular, $A/\mathfrak{m}$ is a field iff it has no nontrivial ideals iff A has no nontrivial ideals containing $\mathfrak{m}$.

In particular, any maximal ideal is prime.

This implies existence of prime ideals in any (nonzero) commutative ring.

4.2.6. **Lemma.** *Any (nonzero) commutative ring has a maximal ideal.*

Proof. Immediate, using Zorn lemma. □

We are now ready to define a "size" of a commutative ring, its (Krull) dimension.

4.2.7. **Definition.** Dimension of a commutative ring A is the greatest number n for which there exists a chain of prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n.$$

The dimension is ∞ if one can find chains of prime ideals of arbitrary length.

For instance, the only prime ideal of a field is 0, thedimension of a field is zero. The dimension of PID (that is not a field) is one.

We will prove later that the dimension of $k[x_1, \ldots, x_n]$ is precisely n. The inequality $\dim(k[x_1, \ldots, x_n]) \geq n$ is obvious as one has a chain of prime ideals defined by the formula $\mathfrak{p}_k = (x_1, \ldots, x_k)$.

4.2.8. An element $a \in A$ is nilpotent if $a^n = 0$ for some n. If $\mathfrak{p}$ is a prime ideal, it contains all nilpotent elements of A. In fact, if $a^n = 0$, $\mathfrak{p} \ni a^n$ so ... $\mathfrak{p} \ni a$.

Definition. Nilradical of A, $N(A)$, is the set of all nilpotent elements of A.

4.2.9. **Proposition.** *$N(A)$ is the intersection of all prime ideals of A.*

Note that this implies that $N(A)$ is an ideal (it is easy however to give a direct proof of this fact).

Proof. Let a be not nilpotent. Denote Σ the set of all ideals of A that do not contain any power of a. Σ is nnonempty as it contains (0). We will verify that Σ satisfies the conditions of Zorn lemma, and that any maximal element in Σ is a prime ideal.

1. Given a chain I_α of elements in Σ let $I = \cup I_\alpha$. This is a nontrivial ideal. and it obviously does not contain any power of a.

2. Let $\mathfrak{p} \in \Sigma$ be a maximal element. Let $bc \in \mathfrak{p}$. if $b \notin \mathfrak{p}$, $(b) + \mathfrak{p}$ contains a power of a. Similarly, if $(c) + \mathfrak{p}$ contains a power of a, $(bc) + \mathfrak{p}$ contains a power of a. This gives a contradiction. □

4.2.10. **Lemma.** *The quotient $A/N(A)$ has no nilpotent elements.*

Proof. If $a + N$ is nilpotent, $a^n \in N$ for some n, so $a^{nm} = 0$ that is $a \in N$. □

4.2.11. *Jacobson radical.* We define the Jacobson radical of A, $J(A)$, as the intersection of all maximal ideals of A.

One has an alternative characterization of $J(A)$.

Proposition. *$x \in J(A)$ iff $1 + xy$ is invertible for all $y \in A$.*

Proof. If $x \in J(A)$, then $1+xy$ does not belong to any maximal ideal. Therefore, this element is invertible. Conversely, if $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, $(x) + \mathfrak{m} = A$, so one can present $1 = xy + z$ with $z \in \mathfrak{m}$. Then $1 - xy = z$ is not invertible. □

One has obviously $J(A) \supset N(A)$ for all A. The important result that we will prove in this course, Hilbert's Nullstellensatz (theorem of zeros) claims that $J(A) = N(A)$ for the rings $A = k[x_1, \dots, x_n]/I$.

(Its importance is not completely obvious. It implies, for instance, that if k is algebraically closed and if $I \neq (1)$, the system of polynomial equations $f(x) = 0$ for all $f \in I$ has a solution in k.)

4.2.12. *Local rings.* A commutative ring A is local if it has only one maximal ideal. Equivalently, A is local if all non-invertible elements form an ideal (this is the unique maximal ideal of A).

As an example, if A is a PID, $A/(a)$ is local iff a power of a prime (this is an exercise).

Some questions about general commutative rings can be reduced to questions about local rings.

4.3. **Operations with ideals.**

4.3.1. *Sum.* If I and J are ideals of A, the sum $I + J$ is the smallest ideal containing both. It is just the sum of the respective additive subgroups. One can also define the sum of any family of ideals.

4.3.2. *Intersection.* Nothing to say: intersection of a family ideals is an ideal.

4.3.3. *Product.* Product of two ideals, I ad J, is the ideal generated by all products xy where $x \in I$ and $y \in J$. One obviously has $IJ \subset I \cap J$.

One can similarly define the product of any finite number of ideals; in partiular, I^n is generated by all products $x_1 \cdots x_n$ with $x_i \in I$.

The ideals I and J are called coprime if $I + J = A$.

Let A be a ring, $I_1, \dots I_n$ be ideals in A. Denote $\phi : A \to \prod_i A/I_i$ the obvious homomorphism.

4.3.4. **Lemma.** 1. *ϕ is injective iff $\cap I_i = 0$.*
2. *ϕ is surjective iff I_i and I_j are coprime for $i \neq j$.*
3. *If I_i are coprime for different i, $\prod I_i = \cap I_i$.*

Proof. The first claim is obvious.

The second claim: assume ϕ is surjective. For some $a \in A$ $\phi(a) = (1, 0, \dots, 0)$, that is, $a = 1 \mod (I_1)$ and $a \in I_2$, so that $1 = (1 - a) + a$ is the required decomposition. In the opposite direction, assume $I_i + I_j = A$, and let us find a such that $\phi(a) = (1, 0, \dots, 0)$. Since I_1 and I_i are coprime for $i \neq 1$, there are decompositions $1 = u_i + v_i$ such that $u_i \in I_1$ and $v_i \in I_i$. Then $\prod v_i$ is 0 modulo I_i for all $i \neq 1$ and $\prod(1 - u_i) = 1 \mod (I_1)$.

The third claim is proven by induction in n. If $n = 2$, $1 = a_1 + a_2$ with $a_i \in I_i$, then for any $x \in I_1 \cap I_2$ we have

$$x = x(a_1 + a_2) = xa_1 + xa_2 \in I_1 I_2.$$

Now, for $n > 2$, assume by induction that $J = \prod_{i=1}^{n-1} I_i = \cap_{i=1}^{n-1} I_i$. We want to verify that $JI_n = J \cap I_n$. We will show that J and I_n are coprime. Choose decompositions of 1, $1 = u_i + v_i$, with $u_i \in I_i$ and $v_i \in I_n$, for any $i \neq n$. Then $\prod u_i = \prod(1 - v_i) = 1 \mod I_n$. This proves the assertion. □

Here is a special property of prime ideals.

4.3.5. **Proposition.** 1. *Let $I \subset \cup_{i=1}^n \mathfrak{p}_i$, $\mathfrak{p}_i$ prime. Then for some i one has $I \subset \mathfrak{p}_i$.*
2. *Let $\mathfrak{p} \supset \cap_{i=1}^n I_i$. Then $\mathfrak{p} \supset I_i$ for some i. If $\mathfrak{p} = \cap I_i$ then $\mathfrak{p} = I_i$ for some i.*

Proof. The first claim. Let $I \not\subset \mathfrak{p}_i$ for all i. We can assume by induction that I is not in the union of all primes but one. Thus, for each i there exists x_i in I but not in $\cup_{j \neq i} \mathfrak{p}_j$. Of course, $x_i \in \mathfrak{p}_i$, so the product $y_i = \prod_{j \neq i} x_i$ belongs to all $\mathfrak{p}_j$, $j \neq i$ but not to $\mathfrak{p}_i$. Then the sum $y = \sum y_i$ does not belong to any $\mathfrak{p}_i$, so $y \notin \cup \mathfrak{p}_i$.

The second claim. Assume $\mathfrak{p} \not\supset I_i$ for all i, then there exist $x_i \in I_i - \mathfrak{p}$. Then the product of x_i is in the intersection of I_i but not in $\mathfrak{p}$. Finally, if $\mathfrak{p} = \cap I_i$ then $\mathfrak{p} \subset I_i$ therefore there is the equality. □

4.4. **Finitely generated modules.** The following result is very important.

4.4.1. **Proposition.** *Let A be a commutative ring, I an ideal in A, M a finitely generated A-module. Assume $f : M \to M$ so that $f(M) \subset IM$. Then there exists a polynomial $p(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ with $a_i \in I$ such that $p(f) = 0$.*

4.4.2. **Remark.** In the special case A a field and $I = 0$ we get a known claim from the linear algebra — it is a cosequence of Cayley-Hamilton theorem.

Proof. We fix a finite sequence of generators $m_1, \ldots, m_n$ of M. One can write

$$f(m_i) = \sum_j c_{ji} m_j,$$

with $c_{ji} \in I$. We will now find an interesting way of interpreting the above equations.

The A-module structure of M can be exteded to the $A[X]$-module structure, if we decide that X acts as the endomorphism $f : M \to M$. We can now rewrite the system of equalities above as

$$\sum_j (c_{ji} - \delta_{ji} \cdot X) m_j = 0.$$

The matrix $A = (c_{ji} - \delta_{ji} \cdot X)$ is an $n \times n$-matrix over the commutative ring $A[X]$. We can multiply it on left with $\mathrm{adj}(A)$ and get the matrix $\det(A)I$. We still get $\det(A)I(m_i) = \det(A)m_i = 0$, that is, $\det(A)M = 0$. It remains to note that $\det(A)$ is a polynomial of degree n of the required form. □

4.4.3. **Remark.** One can use the same way to prove Cayley-Hamilton theorem without using the induction, the passage to algebraic closure of the field, and existence of eigenvectors of an operator over an algebraically closed field. The reason this proof is not usually presented in Linear algebra course — because, to understand it, one has to understand that the notion of determinant works over $k[X]$ in the same way as it works over fields.

4.4.4. **Corollary.** *Let M be f.g., $IM = M$. Then there exists $a \in 1 + I$ such that $aM = 0$.*

Proof. We put $f = \mathrm{id}_M$. □

4.4.5. **Corollary.** *(Nakayama lemma) Let M be f.g., $JM = M$, where J is the Jacobson radical. Then $M = 0$.*

Proof. An element $a \in 1 + J$ is invertible. □

Assume now that A is a local ring with the unique maximal ideal $\mathfrak{m}$. We will now explain that any f.g. A-module has a meaningful notion of a minimal set of generators.

Note that of M is a module over A, $M/\mathfrak{m}M$ is a module over a field $A/\mathfrak{m}$.

4.4.6. **Lemma.** *$A, \mathfrak{m}$ as above, M a f.g. A-module. A collection of elements $m_1, \dots m_n$ of M generated M iff the collection of the images $\bar{m}_1, \dots, \bar{m}_n$ in $\bar{M} = M/\mathfrak{m}M$ generates $\bar{M}$.*

Proof. "Only if" part is obvious. Let N be the submodule of M generated by m_i. Then $N + \mathfrak{m}M = M$, that is, $M/N = \mathfrak{m}M/N$. This implies $M/N = 0$ that is $N = M$. □

4.4.7. **Definition.** Let A be a local rong, M a f.g. A-module. A minimal set of generators of M is a set whose image is a basis in the vector space $M/\mathfrak{m}M$.

In particular, the cardinality of a minimal set of generators of M is $\dim_{A/\mathfrak{m}} M/\mathfrak{m}M$.

4.5. **Hilbert basis theorem.** Recall that a ring is called Noetherian if every its ideal is finitely generated.

4.5.1. **Theorem.** *Let A be a commutative noetherian ring. Then $A[x]$ is also noetherian.*

Proof. Let $I \subset A[x]$ be an ideal. We define J_k as the set of $a \in A$ that appear as a leading coefficient of a degree k polynomial in I. It is easy to see that J_k is an ideal in A and that $J_k \subset J_{k+1}$. We denote $J = \cup J_k$. This is an ideal in A and $J = J_n$ for some n. The ideals J_k, $k = 0, \dots, n$ are finitely generated. Let $a_{k,1}, \dots, a_{k,m_k}$ be generators of J_k. We choose $f_{k,l}$ a degree k polynomial from I with the leading term $a_{k,l}$. We will now prove that the polynomial s $f_{k,l}$ generate I. Let $f \in I$ be a degree d polynomial. We will prove, by induction in d, that f belongs to the ideal generated by $f_{r,s}$. If $d > n$, $J_d = J_n$, so there are $a_1, \dots, a_{m_n}$ such that $f - x^{d-n} \sum a_j f_{n,j}$ is in I and has a smaller degree.

If $d < n$, there are $a_1, \dots, a_{m_d}$ such that $f - \sum a_j f_{d,j}$ is in I and has a smaller degree. This proves the theorem. □

4.5.2. **Corollary.** *Any commutative ring $A = k[x_1, \dots, x_n]/I$ is noetherian.*

Proof. Recall that a ring is noetherian if it is noetherian as a module over itself. Recall as well that a factor of a noetherian module is noetherian. □

4.6. **Rings of fractions.** Let $f : A \to B$ be a ring homomorphism. Define

$$S = \{a \in A | f(a) \text{ is invertible } \}.$$

The S is multiplicatively closed: $1 \in S$ and if $s, t \in S$, then $st \in S$.

In this subsection we will present a construction which allows, for a give multiplicatively closed subset S of a ring A, of a ring homomorphism $f : A \to B$ carrying S to invertible elements of B, and universal in an appropriate sense.

The ring B will be called *the ring of fractions* and will be denoted $S^{-1}A$.

In the special case when A is a domain and $S = A - \{0\}$, we get the fiend of fractions described before.

4.6.1. *Ring of fraction: definition.* Let A be a commutative ring, $S \subset A$ a multiplicatively closed set. A ring of fractions of A with respect to S is a ring homomorphism

$$f : A \to A'$$

carrying S to invertible elements of A' and satisfying the following universal property:

For any ring homomorphism $g : A \to B$ carrying S to invertible elements of B, there exists a unique homomorphism $h : A' \to B$ such that $g = h \circ f$.

A ring of fractions of A with respect to S, if it exists, is unique up to a unique isomorphism.

This is a general property of universal objects.

We will now construct a ring of fractions.

We define $X = A \times S$, the set of pairs (a, s) with $a \in A$ and $s \in S$. We define an equivalence relation on X as follows.

$$(a, s) \sim (b, t) \text{ iff there exists } r \in S \text{ such that } r(at - bs) = 0.$$

It is easy to verify that the above formula defines an equivalence relation. We denote a/s the equivalence class of the pair (a, s).

We can now define the operations on $A' = X/\sim$ by the standard formulas

$$a/s + b/t = (at + bs)/st,\ a/s \cdot b/t = ab/st.$$

One defines $f : A \to A'$ by the formula $f(a) = a/1$.

Let us now verify that the above defined ring homomorphism satisfies the universal property.

Given $g : A \to B$ such that $g(s)$ is invertible for any $s \in S$, we can define $h : A' \to B$ by the formula $h(a/s) = g(a)/g(s)$. The universality is very easy to verify.

The ring of fractions of A with respect to S is usually denoted $S^{-1}A$. Note that $S^{-1}A = 0$ if and only if $0 \in S$.

4.6.2. *Localization.* Given a prime ideal $\mathfrak{p} \subset A$, the complement $S = A \setminus \mathfrak{p}$ is multiplicatively closed.

The ring of fractions $S^{-1}A$, for $S = A \setminus \mathfrak{p}$, is usually denoted $A_{\mathfrak{p}}$. This is a local ring: a/s is not invertible if and only if $a \in \mathfrak{p}$, so $\mathfrak{p}A_{\mathfrak{p}}$ is the unique maximal ideal in $A_{\mathfrak{p}}$.

The ring $A_{\mathfrak{p}}$ is called *the localization of A at $\mathfrak{p}$*.

4.6.3. *Modules over the ring of fractions.* Let $A' = S^{-1}A$ be the ring of fractions. The canonical homomorphism $i : A \to A'$ defines the forgetful functor $i^* : \mathtt{Mod}_{A'} \to \mathtt{Mod}_A$ that identifies $\mathtt{Mod}_{A'}$ with a full subcategory of $\mathtt{Mod}_A$. This means that

- If an A-module has an A'-structure, it is unique. In fact, an A-module M has an A'-structure iff $s : M \to M$ is an automorphism for any $s \in S$. In this case $a/s : M \to M$ is the composition of $a : M \to M$ and of the inverse to $s : M \to M$.
- If M, N are A'-modules, any A-homomorphism from M to N is automatically an A'-homomorphism.

4.6.4. **Lemma.** *Let $S \subset A$ be multiplicatively closed, $I \subset A$ an ideal. Denote $\bar{S} \subset A/I$ the image of S in A/I. Then one has a canonical isomorphism*

$$\bar{S}^{-1}(A/I) = S^{-1}A/S^{-1}I.$$

Proof. The natural homomorphism from A to any of them is universal among ring homomorphisms $A \to B$ carrying the elements of I to zero and the elements of S to invertible elements. □

4.6.5. *Module of fractions.* Similarly, for S, A as above and an A-module M, we define a module of fraction (of M with respect to S) as a homomorphism of A-modules $M \to M'$ such that any $s \in S$ is invertible, when considered as an endomorphism of M', and universal with respect to this property.

Similarly to the above, the module of fractions is unique up to unique isomorphism. It has an explicit construction similar to that of ring of fractions. In more detail, put $Y = M \times S$ and define the equivalence relation by the formula

$$(m, s) \sim (n, t) \text{ iff there exists } r \in S \text{ such that } r(mt - ns) = 0.$$

We denote $M' = Y/\sim$ and denote by m/s the equivalence class of (m, s). The module operations are defined by the formulas

$$m/s + n/t = (tm + sn)/st,\ a/s \cdot m/t = am/st.$$

The map $f : M \to M'$ carries m to $m/1$. The module of fractions of M with respect to S is usually denoted $S^{-1}M$.

4.6.6. *Module of fractions, 2.* The module of fractions $S^{-1}M$ has a canonical structure of $S^{-1}A$-module as, by definition, any $s \in S$ defines an invertible endomorphism of $S^{-1}M$. Therefore, the localization functor can be considered as a functor from $\mathtt{Mod}_A \to \mathtt{Mod}_{A'}$. Moreover,

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}M, N) = \mathrm{Hom}_A(M, N)$$

which means that $S^{-1}M = S^{-1}A \times_A M$.

The above reasoning is a little bit too abstract. A more concrete prove would consist of defining

$$j : S^{-1}A \otimes_A M \to S^{-1}M$$

as the map defined by the bilinear map carrying $(a/s, m)$ to am/s.

4.6.7. **Proposition.** *The localization functor $M \mapsto S^{-1}M$ is exact. That is, given an exact sequence*

$$M \xrightarrow{f} N \xrightarrow{g} K$$

the complex

$$S^{-1}M \xrightarrow{f'} S^{-1}N \xrightarrow{g'} S^{-1}K.$$

Proof. One has $n/s \in \mathrm{Ker}(g')$ iff $g(n)/s = 0$ iff $tg(n) = 0$ for some $t \in S$, that is if $tn \in \mathrm{Ker}(g)$ for some n. Since the original sequence is exact, this is equivalent to saying that there exist $m \in M$ and $t \in S$ such that $f(m) = tn$. The latter means that $n/s = f'(m/st)$. This proves the assertion. □

4.6.8. **Corollary.** *The A-module $S^{-1}A$ is flat.*

Proof. Localization is tensoring by $S^{-1}A$. Since this is an exact functor, $S^{-1}A$ is flat. □

4.6.9. *Local properties.* A property P of a ring is called *local* if A satisfies P iff all localizations $A_{\mathfrak{p}}$ satisfy P. One defines in a similar way locality of a property of a module or of a homomorphism of modules.

4.6.10. **Lemma.** *The following properties of an A-module are equivalent.*

1. $M = 0$.
2. $M_{\mathfrak{p}} = 0$ *for any* $\mathfrak{p}$ *prime.*
3. $M_{\mathfrak{m}} = 0$ *for any* $\mathfrak{m}$ *maximal.*

Proof. Obviously (1) ⇒ (2) ⇒ (3). Let us prove that (3) implies (1). Assume $M \neq 0$. Let $0 \neq m \in M$ and let $I = \mathrm{Ann}(m)$. Choose $\mathfrak{m} \supset I$. The element $m/1 \in M_{\mathfrak{m}}$ should be zero, so there exists $s \notin \mathfrak{m}$ such that $sm = 0$ — contradiction. □

4.6.11. **Lemma.** *Let $f : M \to N$ be an A-module homomorphism. The following is equivalent.*

1. *f is injective (resp., surjective).*
2. *$f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (resp., surjective) for any* $\mathfrak{p}$ *prime.*
3. *$f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp., surjective) for any* $\mathfrak{m}$ *maximal.*

4.6.12. **Lemma.** *The following properties of an A-module are equivalent.*

1. *M is flat.*
2. *$M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module for any* $\mathfrak{p}$ *prime.*
3. *$M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module for any* $\mathfrak{m}$ *maximal.*

The proof of the last two claims is an exercise.

4.6.13. *Behavior of the ideals.* Let $f : A \to B$ be a homomorphism of commutative rings. For J an ideal in B we denote J^c the preimage $f^{-1}(J)$. Conversely, for I an ideal in A we denote I^e the ideal $f(I)B$.

The meaning of the notation: "c" stands for contraction, e for extension.

We denote C the set of contracted ideals of A and E the set of extended ideals of B. Here are the general properties of the contraction / extension operations.

Lemma. 1. *$I \subset I^{ec}$, $J \supset J^{ce}$.*
2. *$J^c = J^{cec}$, $I^e = I^{ece}$.*
3. *$C = \{I | I^{ec} = I\}$, $E = \{J | J^{ce} = J\}$, and the map $I \mapsto I^e$ establishes a bijection between C and E with the inverse $J \mapsto J^c$.*

□

We will now study the contraction and extension operations for a localization $B = S^{-1}A$.

4.6.14. **Proposition.** 1. *Any ideal in $B = S^{-1}A$ is extended.*
2. *For $I \subset A$ one has $I^{ec} = \cup_{s \in S}(I : s)$ where $(I : s) = \{x \in A | sx \in I\}$.*
3. *$I \in C$ iff no $s \in S$ is zero divisor in A/I. In particular, if I is prime, $I \in C$ iff $S \cap I = \emptyset$.*
4. *The prime ideals of B are in one-to-one correspondence with the primes of A that have no intersection with S.*

Proof. 1. Let $J \subset B$ and $x \in J$. One has $x = a/s$ for some $a \in A$ and s. Then $a/1 \in J^{ce}$ and therefore $x = a/s = \frac{1}{s}a/1 \in J^{ce}$.

2. If $x \in (I : s)$ then $sx \in I$ so $x/1 = \frac{1}{s}(sx) \in I^e$, thus, $x \in I^{ec}$. Conversely, if $x \in I^{ec}$ then $x/1 \in I^e$ that is $x/1 = \frac{1}{s}y$ for some $y \in I$. Then $sx \in I$ so $x \in (I : s)$.

3. $I \in C$ iff $I^{ec} = I$ that is $(I : s) = I$ for all $s \in S$.

4. According to the lemma $J \mapsto J^c$ establishes a one-to-one corresondence between C and E. All ideals of B are in E. If J is prime, J^c is prime in A. Conversely, if $I = J^c$ is prime in A, the ideal I^e is prime as $B/I^e = S^{-1}(A/I)$ which has no zero divisors. □

4.6.15. **Corollary.** *The prime ideals of the localization $A_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal of A, are in one-to-one correspondence with the prime ideals of A contained in $\mathfrak{p}$.*

4.6.16. **Lemma.** *The nilradical of $S^{-1}A$ is the extension of the nilradical of A.*

Proof. Obviously, $N(A)^e \subset N(S^{-1}(A))$. It remains to prove that any nilpotent element of $S^{-1}(A)$ belongs to $N(A)^e$. In fact, if a/s is nilpotent, $ta^n = 0$ for some $t \in S$, $n \in \mathbb{N}$. Then $ta \in N(A)$ and $a/s = ta/ts \in N(A)^e$. □

4.7. **Integral dependence.** Let A be a subring of B. An element $b \in B$ is integral over A if it is a root of a polynomial equation

$$x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0$$

with coefficients in A.

Similarly, one can say, for a ring homomorphism $f : A \to B$ that $b \in B$ is integral over A if it is integral over $f(A) \subset B$.

4.7.1. *Example.* Let $x \in \mathbb{Q}$ be integral over $\mathbb{Z}$. We will show that $x \in \mathbb{Z}$. In fact, let $x = \frac{a}{b}$ be a presentation of x as a fraction with $a, b \in \mathbb{Z}$ coprime. Then

$$a^n + \sum_{i=1}^{n} a_i a^{n-i} b^i = 0,$$

which is impossible as a^n is not divisible by b.

4.7.2. *Example.* Let $B = k[t]$ polynomial ring, $A = \mathrm{Span}(1, t^2, t^3 m \ldots) \subset B$. This is obviously a subring in B and $t \in B$ is integral over A as it satisfies the equation $x^2 - t^2 = 0$ with coefficients in A. Note that A and B have the same field of fractions $k(t)$.

4.7.3. **Theorem.** *Let $A \subset B$. The following conditions on $x \in B$ are equivalent.*

1. *x is integral over A.*
2. *$A[x]$, the subring of B generated by A and x, is a f.g. A-module.*
3. *$A[x]$ is contained in a subring C of B that is a f.g. A-module.*
4. *There exists a faithful $A[x]$-module M finitely generated as an A-module.*

Recall that a module is faithful if it is not annihilated by a nonzero element of the ring.

Proof. (1) implies (2). In fact, if $x^n = -\sum_{i=1}^{n} a_i x^{n-i}$, this allows one, by induction, to prove that for any N $x^N \in \mathrm{Span}_A(x^0, \ldots, x^{n-1})$. Thus, $A[x]$ is f.g.

(2) implies (3). Obvious as one can put $C = A[x]$.

(3) implies (4). Obvious as $M := C$ is faithful C-module.

(4) implies (1). In fact, we can apply 4.4.1 to the A-module M and to the endomorphism $\phi : M \to M$ given by multiplication with x. We put $I = A$. We deduce that there exist $a_i \in A$ such that $\phi^n + \sum a_i \phi^{n-1} = 0$ as an endomorphism of M. This endomorphism is given by $x^n + \sum a_i x^{n-1}$. Since M is faithful, this element of $A[x]$ is zero. □

4.7.4. **Corollary.** *If $x_1, \ldots, x_n$ are integral over A then $A[x_1, \ldots, x_n]$ is f.g. A-module.*

Proof. By induction, using that if M is a f.g. B-module and B is a f.g. A-module, then M is a f.g. A-module. □

4.7.5. **Corollary.** *Let B be a finitely generated A-algebra. Then B is integral over A if and only if B is a f.g. A-module.*

□

4.7.6. **Corollary.** *Let $A \subset B$. The set C of elements $x \in B$ integral over A, is a subring of B (it is is called the integral closure of A in B).*

□

If A is the integral closure of A in B, A is called *integrally closed in B*.

A domain A is called integrally closed (or normal) if it is integrally closed in its field of fractions. For instance, $\mathbb{Z}$ is integrally closed.

Actually, any UFD (=unique factorization domain) is integrally closed (Exercise).

4.7.7. **Proposition.** *Let $A \subset B \subset C$. If B is integral over A and C is integral over B then C is integral over A.*

Proof. Let $c \in C$. There exists a polynomial $x^n + \sum b_i x^{n-i}$ in $B[x]$ that vanishes at c. The A-algebra $A[b_1, \dots, b_n]$ is a f.g. A-module and $A[b_1, \dots, b_n, c]$ is a f.g. $A[b_1, \dots, b_n]$-module. Therefore, $A[b_1, \dots, b_n, c]$ is a f.g. A-module containing c. This roves the assertion. □

4.7.8. **Corollary.** *Let C be the integral closure of A in B. Then C is integrally closed in B.*

4.7.9. **Proposition.** *Let $A \subset B$ be an integral extension. Then, for any ideal $J \subset B$ the extension $A/J^c \to B/J$ is integral. Similarly, for any multiplicatively closed $S \subset A$ the map $S^{-1}A \to S^{-1}B$ is integral.*

Proof. The first part is obvious. In the second claim we have to find a polynomial vanishing at b/s, with $b \in B$ and $s \in S$. If b is a root of a polynomial $x^n + \sum a_i x^{n-i}$, b/s is a root of the polynomial $x^n + \sum \frac{a_i}{s^i} x^{n-i}$. □

4.8. **Going-up theorem.** We will now compare chains of prime ideals if A and in B when $A \subset B$ is an integral extension.

4.8.1. **Lemma.** *Let $A \subset B$ be domains, B integral over A. Then A is a field iff B is a field.*

Proof. Let A be a field, $0 \neq x \in B$. The subalgebra $A[x]$ of B is a domain, and is f.g. as A-module. Then multiplication by x is an injective endomorphism of a finitely dimensional vector space over A, therefore, by the Linear algebra version of the pigeon hole principle, is bijective.

Let B be a field, $0 \neq x \in A$. Then x^{-1} is integral over A, so $x^{-n} + \sum a_i x^{i-n} = 0$ for some $a_i \in A$. Multiplying the equality by x^{n-1}, we get the expression of x^{-1} as $-\sum a_i x^{i-1} \in A$. □

4.8.2. **Corollary.** *Let $A \subset B$ be an integral extension, $\mathfrak{q} \in \mathtt{Spec}(B)$, $\mathfrak{p} = \mathfrak{q}^c$. Then $\mathfrak{p}$ is maximal in A iff $\mathfrak{q}$ is maximal in B.*

Proof. Apply the previous lemma to $A/\mathfrak{p} \subset B/\mathfrak{q}$. □

4.8.3. **Corollary.** *Let $A \subset B$ be an integral extension. Let $\mathfrak{q} \subset \mathfrak{q}'$ be prime ideals in B such that $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q}'^c$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Localize A and B at $\mathfrak{p}$. We get an integral extension $A_\mathfrak{p} \subset B_\mathfrak{p}$, the maximal ideal $\mathfrak{p}A_\mathfrak{p}$ and two prime ideals $\mathfrak{q}B_\mathfrak{p}$ and $\mathfrak{q}'B_\mathfrak{p}$ (they are proper ideals as $(A-\mathfrak{p})\cap\mathfrak{q} = \emptyset$ and the same for $\mathfrak{q}'$). The should be both maximal and contain one the other, so they coincide, $\mathfrak{q}B_\mathfrak{p} = \mathfrak{q}'B_\mathfrak{p}$. Therefore, their restrictions to B coincide; we know they give $\mathfrak{q}$ and $\mathfrak{q}'$ respectively. □

4.8.4. **Proposition.** *$A \subset B$ is an integral extension, $\mathfrak{p} \in \mathtt{Spec}(A)$. Then there exists a prime ideal $\mathfrak{q}$ in B such that $\mathfrak{p} = \mathfrak{q}^c$.*

Proof. Localize A and B at $\mathfrak{p}$. We get an integral extension $A_\mathfrak{p} \to B_\mathfrak{p}$. If $\mathfrak{m}$ is a maximal ideal of $B_\mathfrak{p}$, $\mathfrak{m}^c$ is maximal if $A_\mathfrak{p}$, so $\mathfrak{m}^c = \mathfrak{p}A_\mathfrak{p}$. We now define the ideal $\mathfrak{q}$ of B as the restriction of $\mathfrak{m}$. Obviously, its restriction in A is the restriction of $\mathfrak{p}A_\mathfrak{p}$, that is $\mathfrak{p}$. □

And now, the main theorem.

4.8.5. **Theorem.** *(Going-up theorem) Let $A \subset B$ be an integral extension,*

$$\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_n$$

be a chain of prime ideals in A and let

$$\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_m$$

($m < n$) be a partial lifting of this chain to B (that is, $\mathfrak{p}_i = \mathfrak{q}_i^c$). Then one can extend the chain in B to a chain

$$\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_n$$

such that $\mathfrak{p}_i = \mathfrak{q}_i^c$ for all i.

Proof. It is enough to prove the theorem for $n = 1$, $m = 0$. Let $\bar{A} = A/\mathfrak{p}_0$, $\bar{B} = B/\mathfrak{q}_0$. The extension $\bar{A} \subset \bar{B}$ is integral, therefore, by the previous proposition there exists a lifting $\bar{\mathfrak{q}}_1 \subset \bar{B}$ of $\bar{\mathfrak{p}}_1$, the image of $\mathfrak{p}_1$ in $\bar{A}$. It remains to define $\mathfrak{q}_1$ as the preimage of $\bar{\mathfrak{q}}_1$.

□

4.8.6. **Corollary.** *Let $A \subset B$ be an integral extension. Then* $\dim(B) = \dim(A)$.

5. Commutative algebra, II

5.1. **Noether normalization lemma.**

5.1.1. **Theorem.** *Let A be a finitely generated algebra over a field k. Then there exists a subring B of A isomorphic to a polynomial ring $k[x_1, \dots, x_d]$ such that $B \subset A$ is an integral extension.*

We will prove soon that the dimension of $k[x_1, \dots, x_d]$ is precisely d (meanwhile we only know that it is $\geq d$). According to the Going-up Theorem, d in the above theorem is the dimension of A. In other words, for algebras finitely generated over a field, their dimension is the maximal number of algebraically independent elements.

We will only prove the result in the case k is infinite. It remain equally correct for finite fields, but the proof for finite fields is slightly more difficult.

We start with some simple general assertions about infinite fields.

5.1.2. **Lemma.** *Let k be an infinite field and let $f \in k[x_1, \dots, x_m]$ be a nonzero polynomial. The there exist $c_1, \dots, c_m \in k$ such that $f(c_1, \dots, c_m) \neq 0$.*

Proof. Induction in m. For $m = 0$ the claim is vacuous. If $m > 0$, write $f = \sum g_k x_m^k$ where g_k are polynomials in $x_1, \dots x_{m-1}$. There exist k such that $g_k \neq 0$ so there exist $c_1, \dots, c_{n-1}$ such that $f(c_1, \dots, c_{m-1}, x_n)$ is a nonzero polynomial of x_m. Since k is infinite, there exists c_m such that it does not vanish at $x_m = c_m$. □

5.1.3. **Corollary.** *Let k be an infinite field and let $F \in k[x_1, \dots, x_m]$ be a nonzero homogeneous polynomial of m variables.. Then there exist $c_1, \dots, c_{m-1}$ such that $F(c_1, \dots, c_{m-1}, 1) \neq 0$.*

Proof. Let d be the degee of F. Then F/x_m^d is a polynomial in $x_1/x_m, \dots, x_{m-1}/x_m$. The claim follows by applying the previous lemma to this polynomial of $m - 1$ variables. □

Proof of the theorem. Let A be generated over k by $a_1, \dots, a_n$.

Here is an example of why this theorem is not obvious. We could try to define the algebra B as generated over k by a maximal set of algebraically independent generators among a_i. Let, for instance, $A = k[x, y]/(xy)$. The elements x, y generate A, x is algebraically independent (that is, there is no polynomial p in one variable such that $p(x) = 0$ in A), and y is dependent, since $xy = 0$. But y is not integral over $k[x]$ as the xy considered as a polynomial in y is not monic. So, one has to find a clever way of choosing the generators for B.

We will prove the assertion by induction in n. If all a_i are algebraically independent, A is a polynomial ring and there is nothing to prove. Otherwise $a_1, \dots, a_n$ satisfy some nontrivial polynomial equation $f(a_1, \dots, a_n) = 0$, where $0 \neq f \in k[x_1, \dots, x_n]$.

Let $f = \sum_{k=0}^{N} F_k$ where F_k is homogeneous of degree k and $F_N \neq 0$.

Since k is an infinite field, there exist $c_1, \dots, c_{n-1} \in k$ such that $F_N(c_1, \dots, c_{n-1}, 1) \neq 0$.

We put $a'_i = a_i - c_i a_n$ for $i = 1, \dots, n-1$. Obviously, A is generated by $a'_1, \dots, a'_{n-1}, a_n$ and $f(a'_1 + c_1 a'_n, \dots, a'_{n-1} + c_{n-1} a'_n, a'_n) = 0$. Let us decompose the polynomial $f(x_1 + c_1 x_n, \dots, x_{n-1} + c_{n-1} x_n, x_n)$ into homogeneous components. The highest degree component will be $F_N(x_1 + c_1 x_n, \dots, x_{n-1} + c_{n-1} x_n)$. It does not vanish at $(0, \dots, 0, 1)$, so it contains x_n^N as a summand. This implies that in the new coordinates a_n is integral over $k[a'_1, \dots, a'_{n-1}]$. By inductive hypothesis the latter ring is integral over a certain polynomial subring. By transitivity, A is also integral over the same polynomial subring. □

5.2. **Nullstellensatz.** Nullstellensatz is the (German) name of one of celebrated theorems by David Hilbert. The name means "theorem of zeros", and it has to do with existence of solutions of a system of polynomial equations.

Here is the theorem in its simplest form.

5.2.1. **Proposition.** *Let k be algebraically closed, $f_i \in k[x_1, \dots, x_n]$ a collection of polynomials generating a proper ideal $I = (f_i) \neq (1)$. Then there is a solution $(a_1, \dots, a_n) \in k^n$ of the system of equations $f_i(a_1, \dots, a_n) = 0$.*

Proof. Let $A = k[x_1, \dots, k_n]/I$. $A \neq 0$, so, by the normalization lemma there exists a polynomial subring ring $B = k[y_1, \dots, y_m]$ of A such that A is integral over B. Choose any maximal ideal $\mathfrak{n} = (y_1 - b_1, \dots, y_m - b_m)$ in B (for instance, take $b_j = 0$). There is a maximal ideal $\mathfrak{m}$ in A such that $\mathfrak{n} = \mathfrak{m}^c$. The extension $k = B/\mathfrak{n} \to A/\mathfrak{m}$ is integral and finitely generated as algebra. Therefore, its is finite. Thus, $A/\mathfrak{m}$ is a finite field extension of k. Since k is algebraically closed, $A/\mathfrak{m} = k$. Finally, let us consider the preimage J of $\mathfrak{m}$ in $k[x_1, \dots, x_n]$. This is the ideal containing I such that $k[x_1, \dots, x_n]/J = k$. If a_i is the image of x_i under the canonical homomorphism $\rho : k[x_1, \dots, x_n] \to k$, J contains $x_i - a_i$, so $J = (x_1 - a_1, \dots, x_n - a_n)$. The inclusion $J \supset I$ implies that $(a_1, \dots, a_n)$ vanishes at each polynomial $f \in I$. □

5.2.2. **Corollary.** *Let k be algebraically closed. All maximal ideals of $k[x_1, \dots, x_n]$ have form $(x_1 - a_1, \dots, x_n - a_n)$.*

□

And here is a more general formulation.

5.2.3. **Theorem.** *Let k be algebraically closed, $f_i \in k[x_1, \dots, x_n]$ a collection of polynomials generating an ideal $I = (f_i) \neq (1)$. Let $f \in k[x_1, \dots, x_n]$ satisfy the following property.*

For any $a = (a_1, \dots, a_n) \in k^n$, a common zero of all f_i, a is also a zero of f.

Then there exists n such that $f^n \in I$.

Proposition 5.2.1 follows from this theorem. In fact, assuming the elements of I have no common zeros, we apply the theorem to $f = 1$ and deduce that $1 \in I$.

Proof. We will deduce the theorem from Proposition 5.2.1. Let $I = (f_1, \dots, f_m)$. We consider the ideal J in $k[x_0, \dots, x_n]$ generated by $f_1, \dots, f_m$ and $1 - x_0 f$.

The polynomials $f_1, \dots, f_m$ and $1 - x_0 f$ have no common roots, so by 5.2.1 $J = (1)$. That is, there are polynomials $g_0, \dots, g_m \in k[x_0, \dots, x_n]$ such that

$$g_0(1 - x_0 f) + \sum_{i=1}^{m} g_i f_i = 1. \tag{25}$$

This is an equality in $k[x_0, \dots, x_n]$.

Look at the ring homomorphism

$$e : k[x_0, \dots, x_n] \to k[x_1, \dots, x_n]_f \tag{26}$$

(to the ring of fractions) carrying x_0 to $\frac{1}{f}$ and x_i to x_i for $i > 0$.

The homomorphism e carries the left-hand side of (25) to $\sum e(g_i) f_i$, so one has

$$\sum e(g_i) f_i = 1$$

in $k[x_1, \dots, x_n]_f$. after multiplying both sides of the equation with a big enough power of f, we get the required assertion. □

5.3. **Primary ideals.** Recall that a finitely generated module over a PID A has form

$$M = F \oplus M_1 \oplus \dots \oplus M_n$$

where F is free and each one of M_i is *primary cyclic*, that is isomorphic to $A/(p^k)$ where p is a prime element.

A weak form of this theorem for noetherian commutative rings requires a general notion of a primary ideal, something like a power of a prime, but not quite so.

5.3.1. **Definition.** An ideal $\mathfrak{q}$ of a commutative ring A is called *primary* if $\mathfrak{q} \neq A$ and $xy \in \mathfrak{q}$ implies either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some n.

The same can be expressed in terms of $A/\mathfrak{q}$: $\mathfrak{q}$ is primary if and only if any non-zero divisor in $A/\mathfrak{q}$ is nilpotent.

Here are the first properties.

5.3.2. **Lemma.**
1. *Any prime is primary.*
2. *If $\mathfrak{q}$ is primary in B and $A \to B$ is a ring homomorphism then $\mathfrak{q}^c$ is primary in A.*

Proof. The first claim is obvious; the second claim is true as $A/\mathfrak{q}^c$ is isomorphic to a subring of $B/\mathfrak{q}$. □

5.3.3. **Lemma.** *Let $\mathfrak{q}$ be a primary ideal of A and let $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Then $\mathfrak{p}$ is prime (and it is the smallest prime containing $\mathfrak{q}$).*

Proof. if $xy \in \mathfrak{p}$ then $x^n y^n \in \mathfrak{q}$ that is either $x^n \in \mathfrak{q}$ or $y^{nm} \in \mathfrak{q}$. This implies the claim. □

5.3.4. A primary ideal $\mathfrak{q}$ with the radical $\mathfrak{p}$ is called $\mathfrak{p}$-primary. Thus, an ideal $\mathfrak{q}$ is $\mathfrak{p}$-primary iff $xy \in \mathfrak{q}$ implies that either $x \in \mathfrak{q}$ or $y \in \mathfrak{p}$.

5.3.5. *Examples.* Primary ideals are something like powers of primes, but not quite so. Here are a few examples.

1. $A = \mathbb{Z}$, all ideals are principal, a (p)-primary ideal is (p^n). The same answer we have for any PID.
2. $A = k[x, y]$, $\mathfrak{q} = (x, y^2)$. $A/\mathfrak{q} = k[y]/y^2$ so $\mathfrak{q}$ is primary with the radical $\mathfrak{p} = (x, y)$. However, $\mathfrak{q}$ is not a power of $\mathfrak{p}$.
3. Here is an example showing that a power of a prime is not necessarily primary. Let $A = k[x, y, z]/(xy - z^2)$ and $\mathfrak{p} = (\bar{x}, \bar{z})$, where $\bar{a} \in A$ denote the image of $a \in k[x, y, z]$. The quotient $A/\mathfrak{p}$ is isomorphic to $k[y]$, so $\mathfrak{p}$ is prime. On the other hand, $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$ but $\bar{x} \notin \mathfrak{p}^2$ and $\bar{y} \notin \mathfrak{p}$. Therefore, $\mathfrak{p}^2$ is not primary.

The primary ideals whose radical is maximal, are easy to describe.

5.3.6. **Proposition.** *Let $\mathfrak{m}$ be a maximal ideal in A. An ideal $\mathfrak{q}$ is $\mathfrak{m}$-primary iff $\sqrt{\mathfrak{q}} = \mathfrak{m}$.*

Proof. $A/\mathfrak{q}$ has only one prime ideal, $\mathfrak{m}/\mathfrak{q}$. Therefore, it is nilpotent. Thus, any zero divisor in $A/\mathfrak{q}$ is nilpotent, therefore, $\mathfrak{q}$ is primary. □

5.3.7. **Definition.** Let $\mathfrak{p}$ be a prime ideal of A. Its n-th symbolic power, $\mathfrak{p}^{(n)}$ is defined as the restriction of $\mathfrak{p}^n A_{\mathfrak{p}}$ with respect to the localization map $A \to A_{\mathfrak{p}}$.

The ideal $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

5.4. **Krull's theorem.** We are now ready to prove the following important theorem.

For a prime ideal $\mathfrak{p} \in \mathtt{Spec}(A)$ we denote $\operatorname{ht}\mathfrak{p} = \dim(A_{\mathfrak{p}})$ the maximal length of a chain of prime ideals lying in $\mathfrak{p}$.

5.4.1. **Theorem.** *Let A be a noetherian ring, $x \in A$, and let $\mathfrak{p}$ be a minimal prime containing (x). Then* $\operatorname{ht}\mathfrak{p} \leq 1$.

Proof. We assume that, to the contrary, $\operatorname{ht}\mathfrak{p} > 1$. Then there exists a chain of prime ideals $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{q}_0$ in A. We can replace A with $A_{\mathfrak{p}}$ and nothing will change. We can replace A with $A/\mathfrak{q}_0$ and nothing will change.

Thus, we are allowed to assume that $\mathfrak{p}$ is the unique maximal ideal in A and $\mathfrak{q}_0 = 0$, that is, that A is an integral domain.

The ring $A/(x)$ has a unique prime ideal, so it is nilpotent. Since $A/(x)$ is noetherian, the factors $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ have finite length, so $A/(x)$ has a finite length.

Look at the symbolic powers $\mathfrak{q}^{(n)}$. The images of these ideals in $A/(x)$ form a decreasing chain, so it has to stabilize. Therefore,

$$\mathfrak{q}^{(n+1)} + (x) = \mathfrak{q}^{(n)} + (x)$$

for all $n \geq N$ for some N, that is,

$$\mathfrak{q}^{(n)} \subset \mathfrak{q}^{(n+1)} + (x). \tag{27}$$

We will now deduce from this that

$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)}. \tag{28}$$

In fact, left $u \in \mathfrak{q}^{(n)}$. By (27) we can write $u = q + xr$ where $q \in \mathfrak{q}^{(n+1)}$. Then $xr = -q \in \mathfrak{q}^{(n)}$. We have $x \notin \mathfrak{q}$ as $\mathfrak{p}$ is the minimal among the primes containing x. Therefore, $r \in \mathfrak{q}^{(n)}$ as symbolic powers are primary. This implies (28). Finally, put $M = \mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)}$ and deduce that $M = xM$. By Nakayama lemma we have $M = 0$, that is, the symbolic powers $\mathfrak{q}^{(n)}$ stabilize for big n. This is impossible as $A \to A_{\mathfrak{q}}$ is injective, $\mathfrak{q}^{(n)} \subset (\mathfrak{q}A_{\mathfrak{q}})^n$, and these ideals of $A_{\mathfrak{q}}$ have the zero intersection by Nakayama lemma. □

5.4.2. **Corollary.** *Let A be a noetherian ring, $\mathfrak{p}$ a minimal prime containing $I = (x_1, \ldots, x_n)$. Then* $\operatorname{ht}\mathfrak{p} \leq n$.

Proof. We prove the assertion by induction in n. For $n = 0$ $I = 0$, $\mathfrak{p}$ is a minimal prime, so $\operatorname{ht}\mathfrak{p} = 0$. The case $n = 1$ has already been proven. Assume $n \geq 2$. Let us assume that $\operatorname{ht}\mathfrak{p} > n$ so there exists a chain

$$\mathfrak{p} = \mathfrak{p}_{n+1} \supset \ldots \supset \mathfrak{p}_0.$$

If $x_1 \in \mathfrak{p}_1$, we replace A with $A/\mathfrak{p}_1$, and then $\mathfrak{p}/\mathfrak{p}_1$ will be a minimal prime containing $(x_2, \ldots, x_n)$. This will immediately give a contradiction with the inductive hypothesis.

Let us show that we can replace the chain above with another one, having the same length, and satisfying the condition $\mathfrak{p}_1 \ni x_1$. Let us assume that $x_1 \in \mathfrak{p}_k - \mathfrak{p}_{k-1}$. We will show that there exists a prime $\mathfrak{p}'_{k-1}$ between $\mathfrak{p}_k$ and $\mathfrak{p}_{k-2}$, such that $x_1 \in \mathfrak{p}'_{p-1}$. Then, continuing this process, we will get the the chain

$$\mathfrak{p} = \mathfrak{p}_{n+1} \supset \mathfrak{p}'_n \supset \ldots \supset \mathfrak{p}'_1 \supset \mathfrak{p}_0$$

with $\mathfrak{p}'_1 \ni x_1$. This will prove the theorem.

We can replace A with $A_{\mathfrak{p}_k}$ and then factor by $\mathfrak{p}_{k+2}$. We reduce everything to the case of a two-dimensional local domain A with the maximal ideal $\mathfrak{p}_k$ and $\mathfrak{p}_{k+2} = 0$, and an element x_1 in it. Any minimal ideal containing x_1 has height one. Choose any and call it $\mathfrak{p}'_{k-1}$. This proves the claim. □

5.4.3. **Corollary.** $\dim(k[x_1, \ldots, x_n]) = n$.

Proof. First of all, let $\bar{k}$ be an algebraic closure of k. The ring extension

$$k[x_1, \ldots, x_n] \subset \bar{k}[x_1, \ldots, x_n]$$

is integral as all elements of $\bar{k}$ as well as x_i are integral. Therefore, by the Going-Up theorem, the rings have the same dimension.

This reduces the claim to the case k is algebraically closed. In this case, by Nullstellensatz, all maximal ideals are of the form $(x_1 - a_1, \ldots, x_n - a_n)$, in particular, they are generated by n elements. By 5.4.2 the height of any maximal ideal is at most n.

It cannot be less then n as the ideals $\mathfrak{p}_i = (x_1, \ldots, x_i)$, $i = 0, \ldots, n$, form a chain of length n. □

References

[L] S. Lang, Algebra

[AM] M. Atiyah, I. Macdonald, Introduction to commutative algebra.