Commutative algebra

Notation: $A \subset B$ means A is a subset of B, possibly equal to B.

1. Revision

All rings are *commutative rings with unity*.

1.1. Let $f\colon A \to B$ be a ring homomorphism.

Theorem on ring homomorphisms. *The kernel I of f is an ideal of A, the image C of f is a subring of B. The quotient ring A/I is isomorphic to C.*

Proof. Consider the map $g\colon A/I \to C,\ a+I \mapsto f(a)$. It is well defined: $a+I = a'+I$ implies $a-a' \in I$ implies $f(a) = f(a')$.

The element $a+I$ belongs to the kernel of g iff $g(a+I) = f(a) = 0$, i.e. $a \in I$, i.e. $a+I = I$ is the zero element of A/I. Thus, $\ker(g) = 0$.

The image of g is $g(A/I) = \{f(a) : a \in A\} = C$.

Thus, g is an isomorphism. The inverse morphism to g is given by $f(a) \mapsto a+I$.

Correspondence theorem. *Let I be an ideal of a ring A. Then there is a bijection between the set of all ideals J of A such that $I \subset J$ and the set of all ideals of A/I:*

$$\begin{array}{lcl} \{J : I \text{ an ideal of } A,\ I \subset J\} & \longrightarrow & \{K : K \text{ an ideal of } A/I\} \\ J & \longrightarrow & J/I \end{array}$$

Proof. Denote by h the morphism $h\colon A \to A/I,\ a \mapsto a+I$, its image is A/I and its kernel is I.

For an ideal J of A, $I \subset J$, denote by $h|_J\colon J \to A/I, j \mapsto j+I$ the restriction of h to J. Its kernel is I. Similarly to the proof of the previous theorem we deduce that $h|_J(J)$ is isomorphic to J/I which is an ideal of A/I.

For an ideal K of A/I define $K' = h^{-1}(K)$ of A. Then K' is an ideal of A, $I \subset K'$.

Now we have two maps, $J \mapsto J/I$ and $K \mapsto h^{-1}(K)$. They are inverse to each other, i.e. $h^{-1}(J/I) = J$ and $h^{-1}(K)/I = K$. Thus, there is a one-to-one correspondence between the ideals.

1.2. The *intersection* of ideals of A is an ideal of A. Given a subset S of A, one can speak about the minimal ideal of A which contains S. This ideal is equal to

$$\{a_1 s_1 + \cdots + a_m s_m : a_i \in A, s_i \in S, m \geqslant 1\}.$$

Often it is called the ideal *generated by* S.

Let I, J be ideals of a ring A.

Their *sum* $I+J$ is the minimal ideal of A which contains both I and J, more explicitly

$$I + J = \{i + j : i \in I, j \in J\}.$$

Certainly, $I + (J + K) = (I + J) + K$. Similarly one defines the sum of several ideals $\sum I_k$.

Their *product* IJ is the minimal ideal which contains all $ij : i \in I, j \in J$, more explicitly

$$IJ = \{i_1 j_1 + \cdots + i_n j_n : n \geqslant 1, i_m \in I, j_m \in J\}.$$

The product is associative:

$$(IJ)K = I(JK)$$

and distributive:

$$(I + J)K = IK + JK.$$

Similarly one defines the product of several ideals $I_1 \dots I_n$.

Note that $(I + J_1)(I + J_2)$ is the minimal ideal which contains products $(i_1 + j_1)(i_2 + j_2) = (i_1 i_2 + i_2 j_1 + i_1 j_2) + j_1 j_2$, so it is contained in $I + J_1 J_2$:

$$(I + J_1)(I + J_2) \subset I + J_1 J_2,$$

but the inverse inclusion does not hold in general.

For an element a of A the *principal ideal* generated by a is

$$(a) = aA = \{ab : b \in A\}.$$

In particular, $(0) = \{0\}$ is the smallest ideal of A and $(1) = A$ is the largest ideal of A. Unless $A = \{0\}$, these are two distinct ideals of A.

For several elements $a_1, \dots, a_n$ of A the *ideal generated by the* a_i is denoted

$$(a_1, \dots, a_n) = a_1 A + \dots + a_n A = \{a_1 b_1 + \dots + a_n b_n : b_i \in A\}.$$

1.3. A ring A is a *field* if it contains a non-zero element and every non-zero element of A is invertible in A.

Lemma. *A non-zero ring is a field iff it has exactly two different ideals,* (0) *and* (1).

Proof. If I is a non-zero ideal of a field F, then I contains a non-zero element a. Therefore it contains $aa^{-1} = 1$ and therefore it contains $1b = b$ for every b in F; so $I = F$.

Conversely, if a non-zero ring has only two distinct ideals then it is a field: for every nonzero element aA must be equal to (1), hence a multiple of a is 1 and a is invertible.

An ideal I of a ring A is called *maximal* if $I \neq A$ and every ideal J such that $I \subset J \subset A$ either coincides with A or with I. By 1.1 this

equivalent to: the quotient ring A/I has no proper ideals. By the previous lemma this is equivalent to A/I is a field. So we proved

Lemma. *I is a maximal ideal of A iff A/I is a field.*

1.4. A ring A is an *integral domain* if $A \neq 0$ and for every $a, b \in A$ $ab = 0$ implies $a = 0$ or $b = 0$.

Example: every field is an integral domain: $ab = 0$ and $a \neq 0$ implies $b = a^{-1}ab = 0$. $\mathbb{Z}$ is an integral domain. More generally, every non-zero subring of an integral domain is an integral domain.

If A is an integral domain, one can form the *field of fractions* F of A as

$$\{a/b : a \in A, b \in A \setminus \{0\}\}.$$

By definition $a/b = c/d$ iff $ad = bc$.

This is an equivalence relation: if $a/b = c/d$ and $c/d = e/f$ then $ad = bc$ and $cf = ed$ so $adf = bcf = bed$, $d(af - be) = 0$. As d is not zero, $af = be$.

Define two ring operations $a/b+c/d = (ad+bc)/(bd)$ and $(a/b)(c/d) = (ac)/(bd)$. The zero of F is $0/1 = 0/a$ for any non-zero a. Every nonzero element a/b of F is invertible: if $a/b \neq 0$ then $(a/b)^{-1} = b/a$. Thus F is a field. The ring homomorphism $A \to F$, $a \mapsto a/1$ is injective: $a/1 = 0/1$ implies $a = 0$. Thus A can be identified with the subring $A/1$ of F. Then a/b can be identified with ab^{-1} giving the meaning of fraction to the symbol a/b.

Thus, every integral domain is a non-zero subring of a field, and the latter is an integral domain. So the class of integral domains coincides with the class of non-zero subrings of fields.

1.5. An ideal I of a ring A is called *prime* if $I \neq A$ and for every $a, b \in A$ the inclusion $ab \in I$ implies that either $a \in I$ or $b \in I$.

Example: every field has a prime ideal: (0).

Lemma. *I is a prime ideal of A iff A/I is an integral domain.*

Proof. Let I be a prime ideal of A. Let $(a+I)(b+I) = 0+I$, then $ab \in I$. So at least one of a, b is in I which means that either $a+I = 0+I$ or $b+I = 0+I$. Thus, A/I is an integral domain.

Conversely, let A/I be an integral domain. If $ab \in I$ then $(a+I)(b+I) = I = 0+I$, hence either $a+I = I$ and so $a \in I$, or $b+I = I$ and so $b \in I$. Thus, I is a prime ideal of A.

Example: for a prime number p the ideal $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. The zero ideal (0) is a prime ideal of $\mathbb{Z}$.

Corollary. *Every maximal ideal is prime.*

Proof. Every field is an integral domain.

Remark. In general, not every prime ideal is maximal. For instance, (0) is a prime ideal of $\mathbb{Z}$ which is not maximal.

1.6. For rings A_i define their product $A_1 \times \cdots \times A_n$ as the set theoretical product endowed with the componentwise addition and multiplication.

Chinese Remainder Theorem. *Let $I_1, \ldots, I_n$ be ideals of A such that $I_i + I_j = A$ for every $i \neq j$. Then*

$$A/(I_1 \ldots I_n) \simeq \prod_{1 \leqslant k \leqslant n} A/I_k, \qquad a + I_1 \ldots I_n \mapsto (a + I_k)_{1 \leqslant k \leqslant n}.$$

Proof. First let $n = 2$. Then

$$I_1 I_2 \subset I_1 \cap I_2 = (I_1 \cap I_2)A = (I_1 \cap I_2)(I_1 + I_2) \subset (I_1 \cap I_2)I_1 + (I_1 \cap I_2)I_2 \subset I_1 I_2.$$

So $I_1 I_2 = I_1 \cap I_2$. The kernel of the homomorphism

$$A \to \prod_{1 \leqslant k \leqslant 2} A/I_k, \qquad a \mapsto (a + I_1, a + I_2)$$

is $I_1 \cap I_2 = I_1 I_2$. It is surjective: since $I_1 + I_2 = A$, there are elements $x \in I_1, y \in I_2$ such that $x+y = 1$ and hence $bx+ay = a+(b-a)x \in a+I_1$ and similarly $bx + ay \in b + I_2$.

Now proceed by induction on n. Denote $J_1 = I_1, J_2 = I_2 \dots I_n$, so $J_1 J_2 = I_1 \dots I_n$. Since $I_1 + I_k = A$ for all $k > 1$, we deduce using 1.2 that

$$J_1 + J_2 = I_1 + I_2 \dots I_n \supset (I_1 + I_2) \dots (I_1 + I_n) = A,$$

so $J_1 + J_2 = A$. Now in the same way as in the previous paragraph one gets $A/(J_1 J_2) \simeq \prod_{1 \leqslant k \leqslant 2} A/J_k$. By the induction hypothesis $A/J_2 \simeq \prod_{2 \leqslant k \leqslant n} A/I_k$. Thus,

$$A/(I_1 \dots I_n) \simeq \prod_{1 \leqslant k \leqslant n} A/I_k.$$

Example. Let p_i be distinct primes and r_i positive integers. Then

$$\mathbb{Z}/(p_1^{r_1} \dots p_n^{r_n}\mathbb{Z}) \simeq \prod \mathbb{Z}/p_i^{r_i}\mathbb{Z}.$$

2. Modules over rings

2.1. Definition. *Let A be a ring. An abelian group M is called an A-module if there is a multiplication $A \times M \to M$ such that $a(x + y) = ax + ay, (a + b)x = ax + bx, a(bx) = (ab)x, 1x = x$.*

Examples. Every abelian group is a $\mathbb{Z}$-module, so the class of abelian groups coincide with the class of $\mathbb{Z}$-modules.

Every vector space over a field F is an F-module.

2.2. Definition. *A map $f\colon M \to N$ is called a homomorphism of A-modules if $f(x + y) = f(x) + f(y)$ for every $x, y \in M$ and $f(ax) = af(x)$ for every $a \in A$, $x \in M$. A homomorphism f of A-modules is called an*

isomorphism of A-modules, or alternatively an A-isomorphism, if f is bijective.

2.3. Definition. *A subgroup N of an A-module M is called an A-submodule of M if $an \in N$ for every $a \in A, n \in N$.*

Example. Submodules of the A-module A are ideals of A.

Definition. *For an A-module M and its A-submodule N define the quotient module M/N as the quotient set of cosets $m + N$ with the natural addition and multiplication by elements of A.*

Similarly to 1.1 one proves: If M, N are A-modules and $f: M \to N$ is an A-module homomorphism, then the kernel of f is a submodule of M and the image of f is a submodule of N, and $M/\ker(f)$ is A-isomorphic to $\mathrm{im}(f)$.

Similarly to 1.1 submodules of the quotient module M/N are in 1–1 correspondence with submodules of M containing N.

In particular, if $f: M \to N$ is an A-module homomorphism, and K is a submodule of $\ker(f)$, then f induces an A-module homomorphism $g: M/K \to N, \quad m + K \mapsto f(m)$.

2.4. For A-modules M, N the intersection $M \cap N$ is an A-module. So if M, N are contained in a larger module L, one can speak about the minimal A-module which contains a fixed set of elements related to M and N.

Then the

$$M + N = \{m + n : m \in M, n \in N\}$$

is the minimal A-module which contains all all elements of M and N.

Define the direct sum of modules as the set theoretical product with the natural addition and multiplication by elements of A.

Lemma. *Let N, K be A-submodules of an A-module M. A map $f\colon N \oplus K \to N + K$, $f((n,k)) = n + k$ is a surjective A-module homomorpism whose kernel is A-isomorphic to the submodule $N \cap K$. Therefore, if $N \cap K = \{0\}$, $N \oplus K$ is isomorphic to $N + K$.*

Proof. Clearly f is surjective. Its kernel is $\{(n,k) : n + k = 0\}$. Then $n = -k \in N \cap K$. A map $\{(n,k) : n + k = 0\} \to N \cap K, \quad (n,-n) \mapsto n$ is a bijection.

2.5. Definition. *The submodule M generated by elements x_i is the minimal submodule which contains all of them, it consists of finite A-linear combinations of x_i; elements $x_i \in M$ are called generators of M.*

M is said to be of finite type if it has a finite number of generators.

The minimal number of generators (if it exists) of M is called the rank of M.

An A-module M is called free if M has generators x_i such that $\sum a_i x_i = 0$ implies $a_i = 0$ for all i. The set of x_i is called then a basis of M.

2.6. Lemma.

(1) The module $A^n = \oplus_{1 \leqslant i \leqslant n} A$ is free of rank n.

(2) Let M be an A-module of finite type and let $x_1, \ldots, x_n$ be generators of M. Define a homomorphism

$$f\colon A^n \to M, \quad (a_1, \ldots, a_n) \mapsto \sum a_i x_i.$$

It is surjective. If N is the kernel of f, then M is isomorphic to the quotient module $(A)^n/N$. Thus, every A-module of finite type is isomorphic to a quotient of a free module.

(3) Every free module of finite rank n is isomorphic to A^n.

Proof. (1), (2) follow from the definitions. If M is free and the number of generators is finite equal to n, then the homomorphism $(A)^n \to M$ is surjective and injective.

Remark. Similarly to (2) one proves that every A-module is isomorphic to a quotient of a free module.

Elements of N serve as relations for generators of M.

As a corollary we deduce that the direct sum of free modules is free: $A^n \oplus A^m \simeq A^{n+m}$.

Examples. 1. From linear algebra it is known that every module of finite rank over a field has a basis and is free.
2. Let $A = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$ for $n > 1$. Then M has rank 1 and is not a free A-module, since if $M \simeq (\mathbb{Z})^1$ then M would have been infinite.

3. Polylinear constructions

3.1. Definition. *The set of A-module homomorphisms from an A-module M to N is an A-module:* $(af)(m) = a \cdot f(m)$, $(f+g)(m) = f(m)+g(m)$. *It is denoted* $\mathrm{Hom}_A(M, N)$.

Example. Let $A = F$ be a field, and let M be an F-vector space of dimension d_1 and N be an F-vector space of dimension d_2. Fix a basis $\{m_i\}$ in M and a basis $\{n_j\}$ in N. Let C be a matrix of order $d_1 \times d_2$ with entries in F. Define a map $f: M \to N$, $f(\sum a_i m_i) = \sum b_j n_j$ where $(b_1, ..., b_{d_2}) = (a_1, ..., a_{d_1})C$. The map f is an F-linear map. Conversely, every F-linear map $M \to N$ is determined by its values on $\{m_i : 1 \leqslant i \leqslant d_1\}$. Write $f(m_i) = \sum c_{ij} n_j$ and define $C = (c_{ij})$. This gives an inverse map to the previous map. Thus, $\mathrm{Hom}_F(M, N)$ is F-isomorphic to the F-module of matrices of order $d_1 \times d_2$ with entries in F.

Examples–Exercises. $\mathrm{Hom}_A(0, N) = \mathrm{Hom}_A(M, 0) = 0$. $\mathrm{Hom}_A(A, N) \simeq N$,

$\mathrm{Hom}_A(M, N_1 \oplus N_2) \simeq \mathrm{Hom}_A(M, N_1) \oplus \mathrm{Hom}_A(M, N_2)$.

3.2. Definition. *A map* $f\colon M \times N \to R$ *is called* A*-bilinear if for all* $m, m_1, m_2, n, n_1, n_2, a$

$$f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2), \quad f(m, an) = af(m, n)$$

$$f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n), \quad f(am, n) = af(m, n).$$

So for every m *the map* $N \to R, n \mapsto f(m, n)$ *is a homomorphism of* A*-modules and for every* n *the map* $M \to R, m \mapsto f(m, n)$ *is a homomorphism of* A*-modules.*

Note that an A-bilinear map f does not induce a homomorphism of A-modules $M \oplus N \to R$, since $f(a(m, n)) = f(am, an) = a^2 f(m, n)$ is not equal to $af(m, n)$ in general.

Denote the set of all A-bilinear maps $f\colon M \times N \to R$ by $\mathrm{Bil}_A(M, N; R)$. The latter is an A-module with respect to the sum of maps and multiplication of a map by an element of A.

Similarly one can define A-n-linear maps.

Example. Let $A = F$ be a field, and let M be an F-vector space of dimension d_1 and N be an F-vector space of dimension d_2. Fix a basis $\{m_i\}$ in M and a basis $\{n_j\}$ in N. Let C be a matrix of order $d_1 \times d_2$ with entries in F. Define a map $f\colon M \times N \to F$, $f(m, n) = mCn^\circ$ where m is written as a row and n° as a column. The map f is an F-bilinear map. Conversely, every F-bilinear map $M \times N \to F$ is determined by its values on $\{(m_i, n_j) : 1 \leqslant i \leqslant d_1, 1 \leqslant j \leqslant d_2\}$: $f(\sum a_i m_i, \sum b_j n_j) = \sum a_i b_j f(m_i, n_j)$. Now form a matrix C whose entries are $f(m_i, n_j)$. Thus, there is a one-to-one correspondence between bilinear maps $M \times N \to F$ and matrices of order $d_1 \times d_2$ with entries in F.

3.3. To study A-bilinear maps from $M \times N$ to R it is useful to introduce another A-module T and a bilinear map $g\colon M \times N \to T$ such that bilinear maps $f\colon M \times N \to R$ are in one-to-one correspondence with

homomorphisms of A-modules $T \to R$ via g. In other words, we define an isomorphism of A-modules $\mathrm{Bil}_A(M,N;R) \simeq \mathrm{Hom}_A(T,R)$; T does not depend on R but only on A-modules M and N.

Definition of the tensor product. *To define T first denote by L the free A-module with a basis consisting of elements $l_{m,n}$ indexed by elements of $M \times N$. So an arbitrary element of L is a finite sum $\sum a_i l_{m_i,n_i}$ with $a_i \in A$, $m_i \in M$ and $n_i \in N$. Let K be the A-submodule of L generated by elements*

$$l_{m_1+m_2,n} - l_{m_1,n} - l_{m_2,n}, \quad l_{m,n_1+n_2} - l_{m,n_1} - l_{m,n_2},$$
$$l_{am,n} - a l_{m,n}, \quad l_{m,an} - a l_{m,n}$$

(for all $a \in A$, $m \in M$ and $n \in N$).

Denote $T = L/K$. The image of $l_{m,n}$ in T, i.e. the coset $l_{m,n} + K$ is usually denoted by $m \otimes n$.

Since L is generated by $l_{m,n}$, the module T is generated by $m \otimes n$, i.e.

$$T = \Big\{ \sum a_i\, m_i \otimes n_i : a_i \in A, m_i \in M, n_i \in N \Big\}$$
$$= \Big\{ \sum m_i \otimes n_i : a_i \in A, m_i \in M, n_i \in N \Big\}.$$

These satisfy relations:

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \quad (am) \otimes n = a(m \otimes n),$$
$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \quad m \otimes (an) = a(m \otimes n)$$

(for all $a \in A$, $m \in M$ and $n \in N$).

The module T is denote $M \otimes_A N$ and is called the tensor product of M and N over A.

If M, N are finitely generated A-modules, with generators m_i, n_j, then $M \otimes_A N$ is a finitely generated A-module with generators $m_i \otimes n_j$.

We have $n \otimes 0 = 0(n \otimes 1) = 0$.

Now define a map $g\colon M \times N \to M \otimes_A N$ by $(m,n) \mapsto m \otimes n$. It is an A-bilinear map.

3.4. Theorem. *For an* A*-bilinear map* $f: M \times N \to R$ *define* $f': M \otimes_A N \to R$ *as* $f'(\sum a_i m_i \otimes n_i) = \sum a_i f(m_i, n_i)$. *It is a well defined map and it is a homomorphism of* A*-modules. The correspondence* $f \mapsto f'$ *is an isomorphism of* A*-modules* $\mathrm{Bil}_A(M, N; R)$ *and* $\mathrm{Hom}_A(M \otimes_A N, R)$.

Proof. Extend f to a homomorphism $L \to R$ defined on elements of the basis of L by $l_{m,n} \mapsto f(m, n)$.

Since f is bilinear, all generators of K are mapped to zero, so we get $f' = \alpha(f): M \otimes_A N \to R$, $f'(\sum a_i m_i \otimes n_i) = \sum a_i f(m_i, n_i)$. The map α is a homomorphism of A-modules.

Conversely, if $f': M \otimes_A N \to R$ is a homomorphism of A-modules, then define $f = \beta(f'): M \times N \to R$ as $f(m, n) = f' \circ g(m, n)$. Then f is an A-bilinear map.

Now $\alpha \circ \beta(f') = \alpha(f' \circ g)$ and so $\alpha \circ \beta(f')(\sum a_i m_i \otimes n_i) = \sum a_i f' \circ g(m_i, n_i) = f'(\sum a_i m_i \otimes n_i)$. We also have $\beta \circ \alpha(f)(m, n) = \alpha(f) \circ g(m, n) = \alpha(f)(m \otimes n) = f(m, n)$.

Thus, α and β are isomorphisms.

Thus, using the tensor product one can reduce the study of bilinear maps to the study of linear maps.

Example. Let $A = F$ be a field. Let M, N be two F-vector spaces of dimensions d_1 and d_2. In accordance with the previous theorem the vector space of linear maps $M \otimes_F N \to F$ is isomorphic to the vector space of bilinear maps $M \times N \to F$. In accordance with Example in 3.2 the dimension of the space $\mathrm{Bil}(M, N; F)$ is $d_1 d_2$; if $m_1, \ldots, m_{d_1}$ is a basis of M and $n_1, \ldots, n_{d_2}$ is a basis of N, then every bilinear map $f: M \times N \to F$ is determined by its values on $\{(m_i, n_j)\}$.

Therefore, the dimension of the vector space $\mathrm{Hom}_F(M \otimes_F N, F)$ is $d_1 d_2$. It is known from linear algebra that the dimension of a vector space V equals to the dimension of $\mathrm{Hom}_F(V, F)$. So the dimension of

$M \otimes_F N$ is $d_1 d_2$; the F-vector space $M \otimes_F N$ has a basis $m_i \otimes n_j$, $1 \leqslant i \leqslant d_1, 1 \leqslant j \leqslant d_2$.

Note that in the particular case of $M = N$ the space $N \otimes_F N$ has dimension equal to the square of the dimension of N. In physics, N over $F = \mathbb{C}$ represents the state vector of a particle, and $N \otimes_{\mathbb{C}} N$ represents the state vectors of two independent particles of the same kind.

3.5. First properties of the tensor product:

Lemma. (i) $M \otimes_A A \simeq M$,

(ii) $M \otimes_A N \simeq N \otimes_A M$,

(iii) $(M \otimes_A N) \otimes_A R \simeq M \otimes_A (N \otimes_A R)$,

(iv) $M \otimes_A (N \oplus R) \simeq (M \otimes_A N) \oplus (M \otimes_A R)$,

(v) $\mathrm{Hom}_A(M \otimes_A N, K) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, K)) \simeq \mathrm{Hom}_A(N, \mathrm{Hom}_A(M, K))$.

Proof. To prove (i) we first define an A-homomorphism $f\colon L \to M, l_{m,a} \mapsto am$ where L is a free A-module with a basis $l_{m,a}$, $m \in M, a \in A$. Then K (which is the submodule of L defined as in 3.3) is in the kernel of f. So f induces an A-homomorphism $g\colon M \otimes_A A = L/K \to M$, $m \otimes a \mapsto am$. Define $h\colon M \to M \otimes_A A, m \mapsto m \otimes 1$. Then g and h are inverse to each other.

To prove (ii) use an A-homomorphism $f\colon M \otimes N \to N \otimes M, m \otimes n \mapsto n \otimes m$ which corresponds to a map $l_{m,n} \mapsto n \otimes m$ and an A-homomorphism $g\colon N \otimes M \to M \otimes N, n \otimes m \mapsto m \otimes n$. f and g are inverse to each other.

To prove (iii) use $m \otimes (n \otimes r) \mapsto (m \otimes n) \otimes r, (m \otimes n) \otimes r \mapsto m \otimes (n \otimes r)$.

For (iv) use $m \otimes (n, r) \mapsto (m \otimes n, m \otimes r)$, $(m_1 \otimes n, m_2 \otimes r) \mapsto m_1 \otimes (n, 0) + m_2 \otimes (0, r)$.

For (v) use $h \in \mathrm{Hom}_A(M \otimes_A N, K) \mapsto h' \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, K))$, $h'(m)(n) = h(m \otimes n)$ and $h' \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, K)) \mapsto h \in \mathrm{Hom}_A(M \otimes_A N, K)$, $h(m \otimes n) = h'(m)(n)$.

3.6. Examples.

(1) $A^n \otimes_A A^m = A^{nm}$.

(2) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = 0$. Indeed,

$p/q \otimes (n+m\mathbb{Z}) = m(p/qm) \otimes (n+m\mathbb{Z}) = p/(qm) \otimes (mn+m\mathbb{Z}) = p/(qm) \otimes 0 = 0.$

Note that $\mathbb{Z}/m\mathbb{Z}$ is not a free $\mathbb{Z}$-module.

(3) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$. Indeed, define $f: m \otimes n \mapsto mn$. It is surjective. If $\sum m_i \otimes n_i \mapsto 0$, then $\sum m_i n_i = 0$. Let q be a least common multiple of denominators of n_i and then $n_i = r_i/q$ for integer r_i. We get $\sum m_i \otimes n_i = \sum m_i r_i \otimes (1/q) = 0$. Thus f is an isomorphism.

3.7. Definition. *The module* $M^\circ = \mathrm{Hom}_A(M, A)$ *is called the* A*-dual module to* M.

We have a bilinear pairing $M \times M^\circ \to A, \quad (m, f) \mapsto f(m)$ which induces a homomorphism $M \otimes_A M^\circ \to A$ and a homomorphism $M \to M^{\circ\circ}$.

Examples. (1) If $A = F$ is a field and M is a finite dimensional vector space over F with a basis e_i, then define $p_i \in M^\circ$ as $p_i(\sum a_j e_j) = a_i$. Then p_i form a basis of M°. So M and M° are of the same dimension. The homomorphism $M \to M^{\circ\circ}$ is injective and surjective in this case.

(2) If $A = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$ then $M^\circ = 0$.

We have a homomorphism

$$\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(N^\circ, M^\circ), \quad f \mapsto (g \mapsto g \circ f).$$

In the case of vector spaces the latter is an isomorphism.

As a corollary of 3.5, (v) we get (substitute $K = A$)

$(M \otimes_A N)^\circ = \mathrm{Hom}_A(M \otimes_A N, A) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, A)) = \mathrm{Hom}_A(M, N^\circ).$

In the case of vector spaces over a field, from the previous we deduce that

$M \otimes_A N \to (M \otimes_A N)^{\circ\circ} = \mathrm{Hom}_A(M, N^\circ)^\circ \to \mathrm{Hom}_A(M^\circ, N)^\circ$

is an isomorphism, which gives a new definition of the tensor product of vector spaces.

In the case where $N = M^\circ$ we conclude that $M \otimes_A M^\circ$ is isomorphic to the space dual to the space of A-linear operators $\mathrm{Hom}_A(M, M)$ of M.

3.8. Extension of the ground ring.

Let B be an A-module which is a ring. For an A-module M define $M_B = B \otimes_A M$ with

$$b\big(\sum a_i(b_i \otimes m_i)\big) = \sum a_i(bb_i) \otimes m_i.$$

This makes M_B a B-module, which is obtained from M by "extension of scalars" $A \to B$.

Examples. 1. To every $\mathbb{R}$-vector space V one associates its comlexification $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$ which is a vector space over $\mathbb{C}$ of the same dimension as the dimension of V over $\mathbb{R}$.

2. For a finitely generated abelian group M the $\mathbb{Q}$-module $M_{\mathbb{Q}}$ is a finite dimensional vector space over $\mathbb{Q}$. Note that if M is torsion (i.e. for every $m \in M$ there is a non-zero integer n such that $nm = 0$) then $M_{\mathbb{Q}} = 0$.

4. Noetherian modules

4.1. Proposition-Definition. *An A-module M is called Noetherian if it satisfies one of the following equivalent conditions:*

(i) every submodule of M is of finite type;

(ii) every increasing sequence of submodules stabilizes;

(iii) every nonempty family of submodules contains a maximal element with respect to inclusion.

Proof. $(i) \Rightarrow (ii)$: if M_n is an increasing sequence of submodules, then consider $\cup M_n$ which is a submodule of finite type = $\sum x_i A$; if all x_i belong to M_m, then $M_m = M_{m+1} = \dots$;

$(ii) \Rightarrow (iii)$: if there is a nonempty family of submodules without a maximal element, then for every submodule in the family there is a submodule which is strictly larger; then one gets a strictly increasing infinite sequence of submodules, a contradiction;

$(iii) \Rightarrow (i)$: let N be a submodule of M and let E be a maximal module in the family of submodules of finite type of N, then for every $x \in N$ the group $E + Ax$ is a submodule of finite type and $E \subset E + Ax$. Thus $E + Ax = E$ and so $N = E$ is a module of finite type.

4.2. Definition. *A ring A is called Noetherian if A is a Noetherian A-module. In other words the conditions of 4.1 hold for A with submodules replaced by ideals.*

4.3. Example. An integral domain is called a *principal ideal domain* if every ideal is principal. Every principal ideal domain is Noetherian; in particular, every field and $\mathbb{Z}$ are Noetherian rings.

Corollary. *Every nonempty family of ideals in a principal ideal domain contains a maximal element.*

4.4. Example. Let A be a ring and let B be the polynomial ring $A[X_1, X_2, \dots]$ of polynomials in infinitely many variables X_i. Then

$$(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \dots$$

is a strictly increasing sequence of ideals of B. Thus, B is not a Noetherian ring.

4.5. Lemma. *If the quotient ring A/I is a Noetherian A-module, then it is a Noetherian A/I-module, i.e. it is a Noetherian ring.*

Proof. By the correspondence theorem A-submodules of A/I are in one-to-one correspondence with A-submodules of A which contain I, the latter being the set of all ideals of A which contain I and by the correspondence theorem it is in one-to-one correspondence with the set of all ideals of A/I.

4.6. Lemma. *Let M be an A-module and N is a submodule of M. Then M is a Noetherian A-module iff N and M/N are.*

Proof. Work with increasing sequences of submodules ((ii) in 4.1. Let M be Noetherian. Then increasing sequences of submodules of N stabilize and so do increasing sequences of submodules of M/N, since they are in 1-1 correspondence with increasing sequences of submodules of M which contain N. This proves one implication.

Let N and M/N be Noetherian and let M_i be an increasing sequence of submodules of M. Then there is i_1 such that $M_i \cap N = M_{i+1} \cap N$ for $i > i_1$ and there is i_2 such that $(M_i + N)/N = (M_{i+1} + N)/N$ for $i > i_2$. Let $i_3 = \max(i_1, i_2)$ and let $i > i_3$. Let $a \in M_{i+1}$. Then $a = b + c$ for some $b \in M_i$ and $c \in N$. So $c \in M_{i+1} \cap N = M_i \cap N \subset M_i$ and hence $a \in M_i$; thus $M_{i+1} = M_i$.

Corollary 1. *If N_i are Noetherian A-modules, so is $\oplus_{i=1}^n N_i$.*

Proof. Induction on n using 4.6 and the property that the quotient module $\oplus_{i=1}^n N_i / \oplus_{i=1}^{n-1} N_i$ is isomorphic to N_n.

Corollary 2. *A homomorphic image of a Noetherian module is Noetherian.*

Corollary 3. *Let A be a Noetherian ring and let M be an A-module of finite type. Then M is a Noetherian A-module*

Proof. Let M have rank n. Then M is a quotient module of A^n. Since A is a Noetherian A-module, so is so is A^n. Hence M as a quotient module of A^n is Noetherian.

4.7. Theorem. *Let A be a Noetherian ring. Then $A[X]$ is a Noetherian ring.*

Proof. Let J be a non-zero ideal of $A[X]$. For $n \geqslant 0$ define

$$J_n = \{a \in A : \quad \text{there is } f(X) = a_0 + \cdots + aX^n \in J\}.$$

Then J_n is an ideal of A. Since $X(a_0 + \cdots + aX^n) = a_0X + \cdots + aX^{n+1}$, we deduce that $J_1 \subset J_2 \subset \ldots$. Since A is Noetherian, we deduce that there is n such that $J_n = J_{n+1} = \ldots$. For $m \leqslant n$ the ideal J_m as an ideal of the Noetherian ring A is finitely generated, let $c_j^{(m)}$ for $1 \leqslant j \leqslant k_m$ be its generators. Denote by $f_j^{(m)}(X) = \cdots + c_j^{(m)}X^m$ any polynomial of this type in J.

Let $f \in J$ be of degree m. If $m > n$, then $f(X) = a_0 + \cdots + aX^m$ and $a \in J_m = J_n$, so there are $a_j \in A$ such that $a = \sum_j a_j c_j^{(n)}$. Then $f(X) - \sum_j (a_j X^{m-n}) f_j^{(n)}$ is a polynomial in J of degree smaller than m.

If $m \leqslant n$, then there are $a_j \in A$ such that $a = \sum_j a_j c_j^{(m)}$. Then $f(X) - \sum_j a_j f_j^{(m)}$ is a polynomial in J of degree smaller than m.

We see that we can decrease the degree of a polynomial on J subtracting from it an appropriate $A[X]$-linear combination of $f_j^{(m)}(X)$. By induction on m we deduce that every polynomial in J is a linear combination with coefficients in $A[X]$ of $f_j^{(m)}(X)$, $0 \leqslant m \leqslant n$, $1 \leqslant j \leqslant k_m$. Thus, J is finitely generated and $A[X]$ is Noetherian.

Remark. Note that the Noetherian ring $A[X]$ is not a module of finite type over A, since $1, X, X^2, \ldots$ are A-linear independent. So $A[X]$ is not a Noetherian A-module.

Corollary. *The polynomial ring $K[X_1, \ldots, X_n]$, where K is a field, is a Noetherian ring. The quotient ring $K[X_1, \ldots, X_n]/I$ of the polynomial ring is a Noetherian ring.*

5. Unique factorization domains

All rings in this section are integral domains.

5.1. Recall that a unit of a ring A is an inverstible element of A. All units $A^\times$ of a ring A form a group with respect to multiplication.

Recall that for non-zero a, b

$(a) \subset (b)$ iff b divides a (i.e. there is $c \in A$ such that $a = bc$).

Hence $(a) = (b)$ iff $aA^\times = bA^\times$. Denote by F the field of fractions of A. Then $(a) = (b)$ iff $ab^{-1} \in F$ belongs to $A^\times$.

Definition. *A non-zero element a of a ring A which is not a unit of A is called a prime element if $a = bc$ implies b is a unit or c is a unit.*

Note: if a is a prime element, then au is a prime element for any unit u.

Exercise: a is a prime element iff the ideal (a) is a maximal element in the family of proper principal ideals of A (call such ideals *maxp*).

Example: if A is a principal ideal ring, then an ideal is a maxp ideal iff it is a maximal ideal.

5.2. Theorem. *Every proper non-zero ideal of a principal ideal domain A is the product of maxp ideals whose collection (counting multiplicities) is uniquely determined.*

Proof. Let (a) be a proper ideal of A. Consider the family of proper ideals of A which contain (a). The Noetherian property of A implies this family contains a maximal element, say (p_1). So (p_1) is a maximal principal ideal of A. Write $a = p_1 a_1$ with $a_1 \in A$. Since p_1 isn't a unit, (a) is properly contained in (a_1). Continue for a_1, get a_2, etc. By 4.3 the chain of ideals $(a_1) \subset (a_2) \subset \ldots$ should stabilize, which means that $(a_n) = A$ for some n (i.e. a_n is a unit of A). Then $(a) = (p_1) \ldots (p_n)$.

Let $(p_1)\dots(p_n) = (q_1)\dots(q_m)$. Since A is a principal ideal domain, (p_1) is a maximal ideal of A, and hence it is a prime ideal of A. From $q_1 \dots q_m \in (p_1)$ we deduce that, say, $q_1 \in (p_1)$. So $(q_1) \subset (p_1)$ and since (q_1) is a maximal ideal of A, $(q_1) = (p_1)$. So, up to a unit of A the product $p_2 \dots p_n$ is equal to $q_2 \dots q_m$, and hence $(p_2)\dots(p_n) = (q_2)\dots(q_m)$. The induction hypothesis implies the uniqueness.

5.3. Definition. *A ring A is called a unique factorization domain if every non-zero element of A is uniquely factorized into a product of prime elements and a unit. Equivalently, every proper non-zero ideal (a) is a product of a uniquely determined collection (counting multiplicities) of maxp ideals.*

Example. Every principal ideal domain is a unique factorization domain.

Recall that *every field, $\mathbb{Z}$ and every polynomial ring $K[X]$ over a field K is a principal ideal domain*.

Indeed, for fields it is clear. For the ring of integers and the polynomial rings over fields one can use *the division algorithm*. Namely, if I is a non-zero proper ideal of such a ring A, then it contains an element $a \neq 0$ whose module $|a|$ is minimal (resp. whose degree is minimal) positive. Now for every $b \in I$ write using the division algorithm $b = ac + q$ with $c \in A$ where $0 \leqslant q = b - ac \in I$ is smaller than $|a|$ (resp. of degree smaller than that of a) or $q = 0$. The former is impossible, so the latter means that $I \subset (a)$, but obviously, $(a) \subset I$, so $I = (a)$ is a principal ideal.

The previous theorem now implies that *every field, $\mathbb{Z}$ and every polynomial ring $K[X]$ over a field K is a unique factorization domain*.

Prime elements of a field F: none; units: all non-zero elements.

Prime elements of $\mathbb{Z}$: $\pm 2, \pm 3, \pm 5, \dots$; units: ± 1.

Prime elements of $K[X]$: irreducible polynomials of positive degree; units: elements of $K^\times$.

5.4. Lemma. *If A is a unique factorization domain. Let p be a non-zero element of A, not a unit of A. Then p is a prime element of A iff (p) is a non-zero prime ideal of A.*

Proof. Since p is not a unit and not zero, the ideal (p) is a proper non-zero ideal of A.

Let p be a prime element. Then from $ab \in (p)$ one deduces that $ab = pc$ and the unique factorization property shows that either a or b is divisible by p, i.e. $a \in (p)$ or $b \in (p)$; thus, (p) is a prime ideal of A.

Let (p) be a prime proper ideal of A. If $p = ab$ then either a or b belongs to (p). If, say, $a = pc$, then $p = pcb$, so $cb = 1$ and b is a unit of A; thus p is a prime element.

5.5. Definition. *Let A be a unique factorization domain. For two elements a, b their gcd is any element c of A such that c divides a and b, and every d which divides a and b divides c. A gcd is unique up to multiplication by a unit of A.*

Equivalently, $d = gcd(a, b)$ iff (d) is the minimal principal ideal of A containing (a, b).

If both a, b are non-zero and non-units, and $a = up_1^{n_1} \dots p_r^{n_r}$ and $b = vp_1^{m_1} \dots p_r^{m_r}$ with units u, v, prime p_i and non-zero m_i, n_i, then $d = wp_1^{l_1} \dots p_r^{l_r}$ where $l_i = \min(n_i, m_i)$ and w is a unit.

Similarly one defines a gcd of several elements.

Lemma. *Let A be a principal ideal domain. Then d is a gcd of a and b iff $(d) = (a) + (b)$.*

Proof. The ideal generated by $gcd(a, b)$ is the minimal principal ideal of A containing $(a, b) = (a) + (b)$, as noted above.

Elements a, b are called *relatively prime* if their gcd is a unit of A. Two elements a, b are relatively prime iff every factorization of a does not

involve a prime element which divides b. In particular, a prime element p is relatively prime with b iff p does not divide b. In principal ideal domains a, b are relatively prime iff $(a, b) = (1)$.

6. Polynomial rings over unique factorization domains

In this section A is a unique factorization domain.

6.1. Definition. *A polynomial $f \in A[X]$ is called primitive if no prime element of A divides all the coefficients of f. In other words gcd of the coefficients of f is a unit of A.*

Lemma. *Every polynomial g in $A[X]$ can be written as af with $a \in A$ and a primitive polynomial f. Here a is a gcd of the coefficients of g.*

6.2. Lemma. *Let K be the quotient field of A. For every non-zero polynomial $f \in K[X]$ there is a non-zero $a \in K$ such that $af \in A[X]$ is primitive.*

Proof. Let $d \in A$ be the product of denominators of all coefficients of f. Then $g = df \in A[X]$. Let e be a gcd of all coefficients of g. Then d/e is the required element $a \in K$.

6.3. Lemma. *The product of two primitive polynomials is primitive.*

Proof. Let p be a prime element of A. Let $f(X) = a_n X^n + \cdots + a_0$ and $g(X) = b_m X^m + \cdots + b_0$ be primitive polynomials. Let r be the minimal number such that p doesn't divide a_r; similarly, s the minimal number such that p doesn't divide b_s. The coefficient c_{r+s} of X^{r+s} of fg is $a_r b_s + \sum_{i<r} a_i b_{r+s-i} + \sum_{j<s} a_{r+s-j} b_j$. Since a_r, b_s are prime to p, p does not divide $a_r b_s$. Since a_i for $i < r$ and b_j for $j < s$ are divisible by p, p doesn't divide c_{r+s}.

6.4. Lemma. *If f, g are primitive polynomials in $A[X]$ and $f = cg$ with $c \in K$, then c is a unit of A.*

Proof. Let $c = a/b$ with relatively prime $a, b \in A$. Then $ag = bf$ and so b divides ag. Since a gcd of the coefficients of g is a unit of A, a gcd of the coefficients of ag is a times a unit u of A. The element b is relatively prime to a and divides au, so b is a unit of A. Similarly, a is a unit of A. Thus, c is a unit of A.

6.5. It is easy to see that the units of the polynomial ring $A[X]$ (i.e. invertible polynomials) are units of A: $A[X]^\times = A^\times$. A polynomial f in $A[X]$ of positive degree is called *irreducible in* $A[X]$ if it is a prime element of $A[X]$, i.e. if from $f = gh$ with $g, h \in A[X]$ it follows that either g or h is a unit of $A[X]$, i.e. belongs to $A^\times$.

Lemma. *Let A be a unique factorization domain and K be the quotient field of A. Let $f \in A[X]$ be a primitive polynomial of positive degree. Then f is irreducible in $A[X]$ iff f is irreducible in $K[X]$.*

Proof. First, if f is irreducible in $K[X]$, and $f = gh$ is its factorization in $A[X]$ then either g or h is of degree zero, and so is an element of A dividing $f(X)$. Since $f(X)$ is primitive, this element is a unit of A. Thus, f is irreducible in $A[X]$.

Now suppose f is irreducible in $A[X]$. Let $f = gh$ with polynomials g, h over K. Using 6.2 let $a, b \in K \setminus \{0\}$ be such that $ag, bh \in A[X]$ are primitive polynomials. Then $abf = agbh$ is a primitive polynomial by 6.3. Since f and abf are primitive polynomials, we deduce from 6.4 that ab is a unit of A. Let $vab = 1$ for $v \in A$. Thus, $f = (vag)(bh)$ is a factorization of f in $A[X]$. Then either the degree of vag (and hence of g) is zero or the degree of bh (and hence of h) is zero. Thus f is irreducible in $K[X]$.

6.6. Theorem. *Let A be a unique factorization domain. Then $A[X]$ is a unique factorization domain. Its units are units of A and its prime elements are prime elements of A and primitive irreducible polynomials over A of positive degree.*

Proof. Let K be the quotient field of A. Recall that the ring $K[X]$ is a unique factorization domain and its prime elements are irreducible polynomials of positive degree over K.

If p is a prime element of A, then from $p = fg$ with $f, g \in A[X]$ it follows that $f, g \in A$; thus p is a prime element of $A[X]$. In 6.5 we saw that irreducible primitive polynomials of positive degree are prime elements of $A[X]$. If h is a polynomial of positive degree and a prime element of $A[X]$, then it should be primitive and irreducible.

Let f be a non-zero polynomial of positive degree in $A[X]$. Write $f = ag$ with some non-zero $a \in A$ and a primitive polynomial g of positive degree. The latter can be factorized in $K[X]$ as $\prod g_i$ with irreducible polynomials $g_i \in K[X]$ of positive degree. In accordance with 6.2 let $a_i \in K^\times$ be such that $a_i g_i$ is a primitive polynomial of positive degree. Since $a_i g_i$ is irreducible in $K[X]$, it is irreducible in $A[X]$ by 6.5. Then $g \prod a_i = \prod (a_i g_i)$ is a primitive polynomial by 6.3. Since g is primitive, $\prod a_i$ is a unit of A by 6.4. Let $v \prod a_i = 1$ for a $v \in A^\times$, then $f = av \prod (a_i g_i)$. If $a = \prod b_i$ is a factorization of a in A, then $f = v \prod b_i \prod (a_i g_i)$ is a factorization of f in the product of prime elements of $A[X]$. We can also factorize non-zero constant polynomials in $A[X]$ into the product of prime elements of A. Thus, every non-zero and non-unit element of $A[X]$ can be factorized into the product of prime elements of A and primitive polynomials of positive degree which are irreducible over A.

If $f = v' \prod b'_i \prod f'_i$ is another factorization of f in $A[X]$, then from the uniqueness of factorization in $K[X]$ we deduce that up to a permutation $f_i = c_i f'_i$ for some $c_i \in K^\times$ and all i. By Lemma 4 all c_i are units of

A. Then from uniqueness of factorization in A we conclude that up to a permutation $b_i = u_i b_i'$ for units u_i of A.

Thus, the set of prime elements of $A[X]$ consists of prime elements of A and primitive polynomials of positive degree which are irreducible over A, and $A[X]$ is a unique factorization domain.

6.7. Examples.
1. Prime elements of $\mathbb{Z}[X]$: $\pm 2, \pm 3, \pm 5, \ldots$ and $X, X-1, X+1, \ldots, 2X+1, 2X+3, \ldots, X^2+1, \ldots$. Note that $\mathbb{Z}[X]$ is not a PID (since the ideal $(2, X)$ is not principal). More generally, $\mathbb{Z}[X_1, \ldots, X_n]$, $F[X_1, \ldots, X_n]$ (F is a field) are unique factorization domains.
2. Prime elements of $F[X][Y]$: irreducible polynomials in $F[X]$ and irreducible polynomials $f(X,Y) = g_0(X) + g_1(X)Y + \cdots + g_n(X)Y^n$ in $F[X,Y]$, $n > 0$, such that $(g_0(X), \ldots, g_n(X)) = F[X]$. Note that $F[X][Y]$ is not a PID.

6.8. Reduction criterion of irreducibility. *Let A be a unique factorization domain and p a prime element of A. Let $f(X) \in A[X]$ be a primitive polynomial of positive degree whose leading coefficient is not divisible by p. Denote the image of $f(X)$ in $A[X]/pA[X]$ by $\overline{f}(X)$. If $\overline{f}(X)$ is irreducible in $F[X]$ then $f(X)$ is an irreducible polynomial in $A[X]$.*

Proof. If $f = gh$ with polynomial g, h over A of positive degree then their leading coefficients are not divisible by p. So the degree of f, g, h equals the degree of $\overline{f}$, $\overline{g}$, $\overline{h}$. Hence $\overline{f} = \overline{g}\overline{h}$ is a factorization with polynomials $\overline{g}$, $\overline{h}$ of positive degree, a contradiction.

Example. $X^2 + X + 1$ has no roots in $\mathbb{Z}/2\mathbb{Z}$, hence it is irreducible over $\mathbb{Z}/2\mathbb{Z}$. Then for integers n, l, k if the polynomial $(2n+1)X^2 + (2l+1)X + (2k+1)$ is primitive then it is irreducible in $\mathbb{Z}[X]$.

6.9. Eisenstein criterion of irreducibility. *Let p be a prime element of A. Let*

$$f(X) = a_n X^n + \cdots + a_0 \in A[X],$$

be a primitive polynomial of positive degree. Assume that a_n isn't divisible by p, $a_{n-1}, \ldots, a_0$ are divisible by p and a_0 isn't divisible by p^2. Then $f(X)$ is an irreducible polynomial in $A[X]$ and in $K[X]$.

Proof. If $f = gh$ with polynomials g, h over A then their leading coefficients are not divisible by p. Let $g(X) = b_m X^m + \cdots + b_0$ and $h(X) = c_l X^l + \cdots + c_0$. Since $a_0 = b_0 c_0$ is divisible by p and not by p^2, only one, say b_0 is divisible by p and c_0 is relatively prime to p. Let $s \geqslant 0$ be the smallest integer such that b_s is not divisible by p. Then $a_s = b_s c_0 + \sum_{0<i<s} b_i c_{s-i} + b_0 c_s$ isn't divisible by p, so $s = n$ and the degree of g is n, and that of h is zero. Thus, f is irreducible.

Example. $X^n + pX^{n-1} + \cdots + pX + p$ is irreducible over $\mathbb{Z}$ by Eisenstein's criterion whereas the reduction criterion is not applicable to it.

7. Modules over principal ideal domains

Everywhere in this section A is a principal ideal domain.

7.1. Lemma. *(1) $M_k(A)^\times$ consist of matrices whose determinant is a unit of A.*

(2) Let $x_1, \ldots, x_k$ be generators (a basis) of an A-module M. Then for every matrix $T \in M_k(A)^\times$ elements $y_1, \ldots, y_k$ given by

$$\begin{pmatrix} y_1 \\ \ldots \\ y_k \end{pmatrix} = T \begin{pmatrix} x_1 \\ \ldots \\ x_k \end{pmatrix}$$

are generators (resp. a basis) of M.

Proof. (1) If $T \in M_k(A)^\times$ then $TT' = E$ for some $T' \in M_k(A)$. So $\det(T)\det(T') = 1$, and $\det(T) \in A^\times$. Conversely, let $\det(T) \in A^\times$. Recall that the inverse matrix T' of a nonsingular matrix T can be found by a formula

$$T' = \det(T)^{-1}(a_{ij})$$

where the entry a_{ij} of the adjugate to T matrix is $(-1)^{i+j}$ times the determinant of the matrix obtained from T by cutting off the i th column and j th row. In particular, since $T \in M_k(A)$, $(a_{ij}) \in M_k(A)$. Now, since $\det(T) \in A^\times$ we conclude $T' \in M_k(A)$.

(2) Since T is invertible in $M_k(A)$, not only elements $y_1, \dots, y_k$ are A-linearly expressible via elements $x_1, \dots, x_k$, but $x_1, \dots, x_k$ are A-linearly expressible via elements $y_1, \dots, y_k$.

7.2. Theorem (On submodules of a free module). *Let M be a free A-module of finite rank n. Let N be a non-zero submodule of M. Then (i) N is free of rank $k \leqslant n$; (ii) M has a basis $x_1, \dots, x_n$ such that $a_1x_1, \dots, a_kx_k$ is a basis of N where a_i are non-zero elements of A such that $(a_1) \supset (a_2) \supset \cdots \supset (a_k) \neq 0$. This sequence of ideals is uniquely determined by N.*

Proof. Existence.

The module M is of finite type over the Noetherian ring A, so it is a Noetherian A-module by Corollary 3 in 4.6. N is its submodule, so it is a Noetherian A-module by Lemma 4.6.

Let $x_1, \dots, x_n$ be a basis of M. Let $y_1, \dots, y_m$ be generators of N. Each of them can be written as a linear combination of x_i with coefficients in A:

$$\begin{pmatrix} y_1 \\ \dots \\ y_m \end{pmatrix} = (a_{ij}) \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}, \quad a_{ij} \in A.$$

Due to the previous lemma one can (by passing to another generators of M and N) multiply (a_{ij}) by invertible matrices in $M_m(A)$ on the left and

invertible matrices in $M_n(A)$ on the right. We aim to show that as a result of such permited transformations the matrix (a_{ij}) can be transformed to the matrix of the form

$$C = \begin{pmatrix} a_1 & 0 & \dots & \dots & \dots \\ 0 & a_2 & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & a_k & \dots \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

with $(a_1) \supset (a_2) \supset \dots \supset (a_k)$.

Note that some of those multiplications correspond to interchange of columns or rows, multiplication of a column or row by a unit of A, and addition of a column (row) with another column (row) multiplied by an element of A.

For a non-zero element a of A define $l(a)$ as the number of prime elements (counting multiplicities) in a factorization of a; this number does not depend on the choice of factorization. a is a unit iff $l(a) = 0$. Put $l(0) = +\infty$.

It easy to see that if d is a gcd of a, b then $l(d) \leqslant \min(l(a), l(b))$. If $(d) \neq (a), \neq (b)$, then $l(d) < \min(l(a), l(b))$.

The proof goes by induction on $\max(m, n)$.

Base of induction. If $\max(n, m) = 1$, the statement is clear, since the matrix (a_{ij}) is 1×1.

Induction step. It is sufficient to prove the following claim: A can be transformed to a matrix $\begin{pmatrix} a_1 & 0 \\ 0 & B \end{pmatrix}$ with a_1 dividing all entries of the matrix B (so that then one applies the induction hypothesis to B, and a_1 will divide the entries of transformed B). The proof of the claim goes by second induction on $l = \min(l(a_{ij}))$.

Let $l = 0$. Then one of a_{ij} is a unit in A. By interchanging rows and columns one can assume that $i = j = 1$. So a_{11} divides all other elements of the matrix. By subtracting from the ith row the first row multiplied by

$a_{i1}a_{11}^{-1}$ and by similar operation with the columns we can transform the original matrix to a new one (denote it still by (a_{ij}) whose entries in the first row and column except a_{11} are zero and a_{11} divides all other entries.

Let $l > 0$. Using the induction hypothesis (on l) we can assume that no permitted transformation of the matrix (a_{ij}) makes its number l strictly smaller.

One can assume without loss of generality that $l = l(a_{11})$. If a_{11} doesn't divide some a_{1j} or some a_{i1}, say a_{12}, then let d be a gcd of a_{11} and a_{12} and let $e, f \in A$ be such that $ea_{11}/d + fa_{12}/d = 1$. Let

$$T = \begin{pmatrix} e & -a_{12}/d & 0 \\ f & a_{11}/d & 0 \\ 0 & 0 & E \end{pmatrix}.$$

The matrix T has determinant 1 and

$$(a_{ij})T = \begin{pmatrix} d & 0 & \dots \\ \dots & \dots & \dots \end{pmatrix}.$$

Since $l(d) < l(a_{11}) = l$, we get a contradiction.

So a_{11} must divide all a_{1j} and a_{i1}. By subtracting from the ith row the first row multiplied by $a_{i1}a_{11}^{-1}$ and by similar operation with the columns we can transform the original matrix to a new one (denote it still by (a_{ij}) whose entries in the first row and column except a_{11} are zero and $l = l(a_{11})$ is still the minimum of $l(a_{ij})$.

If a_{11} doesn't divide some a_{ij} with $i, j \geqslant 2$, then add to the first row the ith row which puts a_{ij} in place $1j$. Repeating the previous argument we get a contradiction.

Thus, both in case $l = 0$ and $l > 0$ $a_1 = a_{11}$ divides all a_{ij} and entries in the first row and column except a_{11} are zero.

Thus, M has a basis $x_1, \dots, x_n$ such that N is generated by $a_1x_1, \dots, a_kx_k$. Clearly $k \leqslant n$. From $\sum c_i(a_ix_i) = 0$ one deduces $c_ia_i = 0$ (since x_i is a basis of M) and hence $c_i = 0$. Thus, $a_1x_1, \dots, a_kx_k$ form a basis of N.

Uniqueness. Let d_i be a gcd of the i-rowed minors of (a_{ij}). Since the rows (resp. columns) of $T(a_{ij})$ (resp. $(a_{ij})T$) are linear combinations of rows (resp. columns) of (a_{ij}), d_i divides a gcd of the i-rowed minors of $T(a_{ij})$ and of $(a_{ij})T$. Since T is invertible, we conclude that $d_i((a_{ij}))A^\times = d_i(C)A^\times$. Since the i-rowed minors of C is $a_1 \dots a_i$, we deduce that

$$d_i(C) = a_1 \dots a_i u = a_i d_{i-1}(C)v$$

for units u, v. Thus a_i are equal up to a unit of A to $d_i((a_{ij}))/d_{i-1}((a_{ij}))$. So (a_i) are uniquely determined by the submodule N.

7.3. The Main Theorem on modules of finite type over a principal ideal domain. *Let A be a principal ideal domain. Let $R \neq 0$ be an A-module of finite type. Then*

$$R \simeq A/I_1 \oplus \dots \oplus A/I_n$$

where $I_1 \supset \dots \supset I_n$ are proper ideals of A (some of which may be zero) uniquely determined by R.

Proof. Let $r_1, \dots, r_n$ be a minimal set of generators of R. By 2.6 there is a surjective homomorphism $f\colon (A)^n \to R$ so that R is isomorphic to $(A)^n/N$ where N is the kernel of f. Let $M = (A)^n$; apply the previous theorem. Put $a_i = 0$ for $i > k$ and $I_i = a_i A$. So the sequence of the ideals $I_1, \dots, I_n$ is uniquely determined by R.

Define a map

$$g\colon \oplus A/a_iA \to (\oplus x_iA)/(\oplus a_ix_iA), \quad (b_i + a_iA) \mapsto (x_ib_i) + \oplus a_ix_iA.$$

It is an isomorphism. Thus,

$$R \simeq (A)^n/N \simeq (\oplus x_iA)/(\oplus a_ix_iA) \simeq \oplus A/a_iA = \oplus A/I_i.$$

Example. Finitely generated abelian groups: every such group is isomorphic to $\oplus_i \mathbb{Z}/a_i\mathbb{Z} \oplus (\mathbb{Z})^{n-k}$ with a_1 dividing a_2 dividing a_3, ..., dividing $a_k \neq 0$.

7.4. Corollary. *Every module of finite type over a principal ideal domain is isomorphic to the direct sum* $\oplus M_i$ *of modules* M_i *where* $M_i = A$ *or* $M_i = A/p^m A$ *where* p *is a prime element of* A.

Proof. If $I_1 = (a_1)$ and $a_1 = \prod p_i^{r_i}$ with prime p_i then by the Chinese Remainder Theorem in 1.5 we have $A/I_1 \simeq \prod A_i/p_i^{r_i} A$.

7.5. Definition. *A module* M *over an integral domain* A *is torsion free if* $am = 0$ *implies* $a = 0$ *or* $m = 0$.

Examples. $(A)^n$ is torsion free; A/I is not torsion free if $I \neq 0,\ I \neq A$.

Corollary. *Every torsion free module of finite type over a principal ideal domain is free.*

Proof. Indeed, if R is a torsion free module of finite type then all I_k in theorem 8.3 must be zero, so $R \simeq A^n$ is free.

Exercise. $\mathbb{Q}$ is a torsion free $\mathbb{Z}$-module and is not free. Of course, $\mathbb{Q}$ is not of finite type over $\mathbb{Z}$.

8. Spectrum of rings

8.1. One can try to study a ring A by looking at all of its surjective images in integral domains, which is equivalent to looking at all prime ideals of A. Alternatively one can study A by looking at all of its surjective images in fields, which is equivalent to looking at all maximal ideals of A.

Definition. *The spectrum* Spec (A) *of a ring* A *is the set of prime ideals* P *of* A. *The maximal spectrum m-Spec(* A*) of a ring* A *is the set of maximal ideals* M *of* A.

8.2. Examples. 1. Spec of a field consists of one element – the zero ideal (0).

2. Spec $(\mathbb{Z})$ is in one-to-one correspondence with all positive prime numbers and 0.

3. If A is a principal ideal domain, then Spec (A) consists of the zero ideal and the principal prime ideals (a) where a are prime elements of A.

If K is a field, then Spec $(K[X])$ consists of the zero ideal and principal ideals generated by monic irreducible polynomials.

In particular, elements of Spec $(\mathbb{C}[X])$ different from $\{0\}$ (i.e. elements of the max spectrum m-Spec $(\mathbb{C}[X])$) are one-to-one correspondence with complex numbers.

4. If A is a principal ideal domain, then it can be shown that Spec $(A[X])$ consists of the zero ideal, principal ideals generated by irreducible polynomials $f(X)$ and maximal ideals $M = (p, q(X))$ generated by two elements, where p is a prime element of A and the reduction of $q(X)$ modulo p is an irreducible polynomial over A/pA.

8.3. Let $f: A \to B$ be a homomorphism of rings. Let P be a prime ideal of B. Then its preimage $f^{-1}(P)$ is a prime ideal of A (note that $1_B \notin P$ implies $1_A \notin f^{-1}(P)$). So we get a map of sets

$$f^*: \text{Spec}\,(B) \to \text{Spec}\,(A), \quad P \mapsto f^{-1}(P).$$

Examples: Spec $(\mathbb{Z}/p\mathbb{Z}) \to$ Spec $(\mathbb{Z})$, Spec $(\mathbb{Z}[i]) \to$ Spec $(\mathbb{Z})$.

Let M be a maximal ideal of B. Then $f^{-1}(M)$ isn't necessarily a maximal ideal of A.

Example: $f: \mathbb{Z} \to \mathbb{Q}$, $f^{-1}(\{0\}) = \{0\}$.

However, if f is surjective, then $A/f^{-1}(M) \simeq B/M$, so $f^{-1}(M)$ is a maximal ideal of A.

It is more natural to work with Spec rather than with m-Spec even though the latter is more naturally related with analytic and geometric objects.

8.4. Geometric interpretation of spectrum. Let I be an ideal of $\mathbb{C}[X_1, \ldots, X_n]$. The set $V = V(I)$ of all solutions of polynomial equations $f(X_1, \ldots, X_n) = 0$, $f \in I$ is called an *algebraic variety*.

For a subset X of $\mathbb{C}^n$ consider the set of all polynomials $g \in \mathbb{C}[X_1, \ldots, X_n]$ for which $g(X) = 0$. It is an ideal of $\mathbb{C}[X_1, \ldots, X_n]$ and called the ideal $J(X)$ of the set X.

So one has two maps:

V: ideals of $\mathbb{C}[X_1, \ldots, X_n] \to$ algebraic varieties of $\mathbb{C}^n$,

J: subsets X of $\mathbb{C}^n \to$ ideals of $\mathbb{C}[X_1, \ldots, X_n]$.

We have $J(X_1) \subset J(X_2)$ if $X_1 \supset X_2$ and $V(I_1) \subset V(I_2)$ if $I_1 \supset I_2$, $J(\emptyset) = \mathbb{C}[X_1, \ldots, X_n]$, $J(V(I)) \supset I$, $V(J(X)) \supset X$.

Definition. *For an ideal I its radical $\sqrt{I}$ is the set of elements a of A such that $a^n \in I$ for some $n > 0$.*

Then $\sqrt{I}$ is an ideal: if $a^n, b^m \in I$ then $(a+b)^{n+m} \in I$. If I is prime then $\sqrt{I} = I$.

Hilbert theorem on zeros. *$J(V(I)) = \sqrt{I}$. In particular, if I is prime then $J(V(I)) = I$.*

An algebraic variety X is called *irreducible* if $X = V(I)$ for a prime ideal I.

Theorem. *The maps V, J induce a 1-1 correspondences between* Spec $(\mathbb{C}[X_1, \ldots, X_n])$ *and irreducible algebraic varieties of $\mathbb{C}^n$.*

They induce a 1-1 correspondence between m-Spec $((\mathbb{C}[X_1, \ldots, X_n])$ *and points of $\mathbb{C}^n$.*

Proof. The previous theorem implies that if an algebraic variety V is irreducible $= V(I)$ for a prime ideal I, then $J(V) = I$ is a prime ideal. We also have $V(J(V(I)) = V(I)$ if I is a prime ideal. Hence the maps V

and J are 1-1 correspondences between

Spec $(\mathbb{C}[X_1, \ldots, X_n])$ and irreducible algebraic varieties of $\mathbb{C}^n$.

To prove the second part we need to describe the image of maximal ideals.

If x is a point of $\mathbb{C}^n$, then the map

$$\mathbb{C}[X_1, \ldots, X_n] \to \mathbb{C}, \quad f \mapsto f(x)$$

is a surjective homomorphism whose kernel M_x consists of polynomials which have x as a zero. Thus, M_x is a maximal ideal of $\mathbb{C}[X_1, \ldots, X_n]$. Obviously $x \in V(M_x)$. Since for $y \neq x$ there is a polynomial f such that $f(x) = 0 \neq f(y)$ and we deduce $V(M_x) = \{x\}$.

The map $x \mapsto M_x$ is injective: as we have seen, if $x \neq y$ then $M_x \neq M_y$.

Let's show that the image of the map $x \mapsto M_x$ coincides with the set of all maximal ideals of $\mathbb{C}[X_1, \ldots, X_n]$. If M is a maximal ideal then $V(M)$ is not empty, since by the Hilbert theorem $J(V(M)) = M \neq \mathbb{C}[X_1, \ldots, X_n] = J(\emptyset)$. Let $x \in V(M)$ then $M_x = J(\{x\}) \supset J(V(M)) = M$, hence since the LHS and RHS are maximal ideals, $M_x = M$.

Thus, $\mathrm{m} - \mathrm{Spec}((\mathbb{C}[X_1, \ldots, X_n]) = \{M_x\}$ and its image with respect to V are all points of $\mathbb{C}^n$.

8.5. For an algebraic variety V define the ring

$$\mathbb{C}[V] = \mathbb{C}[X_1, \ldots, X_n]/J(V).$$

It is called the *ring of polynomial functions* on V. If V is irreducible $\mathbb{C}[V]$ is an integral domain.

If $x \in V$ then $M_x = J(\{x\}) \supset J(V)$. Denote by $\overline{M}_x$ the image of M_x is $\mathbb{C}[V]$, this is a maximal ideal of $\mathbb{C}[V]$. By the correspondence theorem we have a one-to-one correspondence between ideals of $\mathbb{C}[V]$ and ideals of $\mathbb{C}[X_1, \ldots, X_n]$ which contain $J(V)$. Thus, from the previous

theorem we deduce that *for an algebraic variety* V *the maps* V, J *induce a 1-1 correspondence between* m-Spec $(\mathbb{C}[V])$ *and points of* V.

8.6. Analytic interpretation of spectrum. Let X be a bounded closed set in a finite dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$. Denote by $C(X)$ the set of all real continuous functions on X. It is a ring. For $x \in X$ denote by M_x the set of all functions g in $C(X)$ for which $g(x) = 0$. It is a maximal ideal of $C(X)$ as the kernel of the surjective map $C(X) \to \mathbb{R}$, $f \to f(x)$. We have the map

$$\Phi\colon X \to \text{m-Spec}\,(C(X)), \quad x \mapsto M_x.$$

From analysis it is known that for $x \neq y$ there is $f \in C(X)$ such that $0 = f(x) \neq f(y)$, so $f \in M_x, f \notin M_y$ and then $M_x \neq M_y$. Hence Φ is injective.

Let M be a maximal ideal of $C(X)$ and $V = V(M) = \{x \in X : f(x) = 0 \quad \text{for all} \quad f \in M\}$. If V is empty, then for every $x \in X$ there is $f_x \in M$ such that $f_x(x) \neq 0$. Since f_x is continuous, there is a neighbourhood U_x of x where f_x takes only non-zero values. So $X = \cup U_x$. One can deduce that there are finitely many U_x whose union is X. Let $X = U_{x_1} \cup \cdots \cup U_{x_n}$. Consider $f = f_{x_1}^2 + \cdots + f_{x_n}^2$. Then $f \in M$. Since for every $x \in X$ there is f_{x_i} such that $f_{x_i}(x)^2 > 0$ we deduce $f(x) > 0$ for every $x \in X$. So $f^{-1} \in C(X)$. Recall that $f \in M$. Then $1 = ff^{-1} \in M$, a contradiction. Thus, V is non-empty. Take any $x \in V$. Then $M \subset M_x$, so $M = M_x$. Thus, Φ is a bijection and we proved

Theorem. *There is a 1-1 correspondence between points of a bounded closed set* X *in a finite dimensional vector space over* $\mathbb{R}$ *or* $\mathbb{C}$ *and the maximum-spectrum* m-Spec $(C(X))$ *of the ring of all real continuous functions on* X.

9. Localization

9.1. Definition. *Let* A *be a ring and* S *is a subset of* A. S *is called a multiplicative (sub)set if* $1 \in S$ *and* $a, b \in S \Rightarrow ab \in S$.

Examples of a multiplicative sets:

1. $S = A \setminus \{0\}$ is a multiplicative set if A is an integral domain.
2. For a prime ideal P the set $S = A \setminus P$ is a multiplicative set.
3. For $c \in A$ the set $S_c = \{1, c, c^2, \dots\}$ is a multiplicative set.

9.2. Definition. *Let* $0 \notin S$. *Define a relation* $\equiv$ *on* $A \times S$*:*

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

One can think of (a, s) *as* a/s. *Transitivity of the relation: if* $(a, s) \sim (b, t)$ *and* $(b, t) \sim (c, p)$, *then there are* $u, v \in S$ *such that* $(at - bs)u = (bp - ct)v = 0$. *Then* $(ap - cs)tuv = 0$. *Since* $tuv \in S$, *we conclude that* $(a, s) \sim (c, p)$.

Denote by a/s *the equivalence class of* (a, s) *with respect to* $\equiv$. *Let* $S^{-1}A$ *be the set of all equivalence classes. Define the ring structure by* $a/s + b/t = (at + bs)/st$, $(a/s)(b/t) = ab/st$. *The RHS doesn't depend on the choice of representatives. The zero of* $S^{-1}A$ *is* $0/1$ *and the unity is* $1/1$.

The ring $S^{-1}A$ *is called the ring of fractions of* A *with respect to* S.

9.3. Examples.

1) Let A be an integral domain. The equivalence relation then becomes $(a, s) \sim (b, t)$ iff $at - bs = 0$.

If $S = A \setminus \{0\}$ then the ring $S^{-1}A$ is the fraction field of A.

From now on we will assume A *is an integral domain.* Then for every multiplicative subset S of $A \setminus \{0\}$ the ring $S^{-1}A$ is a subring of the fraction field of A.

2) Let P be a prime ideal of A. Then $S = A \setminus P$ is a multiplicative subset of A. The ring

$$A_P = (A \setminus P)^{-1}A = \{r/s : r \in A, s \notin P\}$$

is called the *localization* of A at P; it is a subring of the field of fractions of A. For example,

$$\mathbb{Z}_{(p)} = \{r/s : r, s \in \mathbb{Z}, s \notin p\mathbb{Z}\}$$

is a subring of the field of rational numbers.

3) Geometric interpretation of the localization.

Let V be an irreducible algebraic variety. Then $P = J(V)$ is a prime ideal of $\mathbb{C}[X_1, \ldots, X_n]$ and so $\mathbb{C}[V] = \mathbb{C}[X_1, \ldots, X_n]/J(V)$ is an integral domain.

The localization $\mathbb{C}[X_1, \ldots, X_n]_P$ is a subring of $\mathbb{C}(X_1, \ldots, X_n)$ consisting of rational functions $\{f/g : f, g \in \mathbb{C}[X_1, \ldots, X_n], g \notin P\}$ which are defined on a nonempty subset of V. If $V = \{x\}$ is a point, then P is maximal and $\mathbb{C}[X_1, \ldots, X_n]_P = \{f/g : f, g \in \mathbb{C}[X_1, \ldots, X_n], g(x) \neq 0\}$ consists of rational functions which are defined at x.

9.4. Define a homomorphism

$$\phi\colon A \to S^{-1}A, \quad \phi(a) = a/1.$$

Since we assume A is an integral domain, this map is injective.

We have $\phi(S) \subset (S^{-1}A)^\times$ since $(s/1)(1/s) = 1$. For example, all primes in $\mathbb{Z}$ not divisible by p have their images in the localization $\mathbb{Z}_{(p)}$ as units of the latter ring.

9.5. Proposition. *Every ideal J of $S^{-1}A$ is of the form*

$$S^{-1}I = \{a/s : a \in I, s \in S\},$$

where $I = \phi^{-1}(J)$ is an ideal of A.

Proof. If I is an ideal of A then $S^{-1}I$ is an ideal of $S^{-1}A$.

If J is an ideal of $S^{-1}A$, put $I = \phi^{-1}(J)$; it is an ideal of A.

We have $\phi(I) \subset J$ and hence $S^{-1}I \subset J$.

If $a/s \in J$, then for every $s \in S$ we have $(a/s)(s/1) = a/1 = \phi(a)$, so $\phi(a) \in J$, hence $a \in I$, and $a/s \in S^{-1}I$. Thus, $J \subset S^{-1}I$.

Corollary. *If A is Noetherian, so is $S^{-1}A$.*

9.6. Proposition. *Prime ideals of $S^{-1}A$ are in one-to one correspondence with prime ideals of A disjoint with S:*

$$P, P \cap S = \emptyset \mapsto S^{-1}P,$$
$$Q \mapsto \phi^{-1}(Q).$$

Thus, $\text{Spec}\,(S^{-1}A) = \{PS^{-1}A : P \in \text{Spec}\,(A), P \cap S = \emptyset\}$.

Proof. Let P be a prime ideal of A disjoint with S.

If $1/1$ were equal to $p/s \in S^{-1}P$, then we would have $s = p \in P$ which contradicts $s \in S \subset A \setminus P$.

If $a/s \cdot b/t = p/u$ with $p \in P$, $u \in S$, then $abu = pst \in P$. Since $u \in S$ doesn't belong to P we deduce that $ab \in P$ and therefore either $a \in P$ or $b \in P$. Then either $a/s \in S^{-1}P$ or $b/t \in S^{-1}P$ and the ideal $S^{-1}P$ is prime.

If Q is a prime ideal of $S^{-1}A$, then its preimage $P = \phi^{-1}(Q)$ is a prime ideal of A by 8.3.

From the proof of Proposition 9.5 we get $Q = S^{-1}P$. If $P \cap S \neq \emptyset$, then for $s \in P \cap S$ we would have $1 = s/s \in Q$, a contradiction. Therefore, P is disjoint with S.

It remains to show that maps $\alpha: P \mapsto S^{-1}P$ for $P \cap S = \emptyset$ and $\beta: Q \mapsto \phi^{-1}(Q)$ are inverse to each other. From 9.5 we already know that $\alpha \circ \beta$ is the indentity map. To show $\beta \circ \alpha$ is the indentity map let $a \in \phi^{-1}(S^{-1}P)$. Then $a/1 = p/s$ for some $p \in P, s \in S$. Hence

$as = p \in P$. Since $s \notin P$ and P is a prime ideal, we deduce $a \in P$. Thus $\phi^{-1}(S^{-1}P) = P$.

9.7. Corollary. *Let P be a prime ideal of A. Then the localization A_P has only one maximal ideal, namely $M_P = PA_P$. Thus,* $\text{Spec}\,(A_P) = \{QA_P : Q \in \text{Spec}\,(A), Q \subset P\}$, $\text{m-Spec}\,(A_P) = \{PA_P\}$.

Proof. Indeed, prime ideals of A_P correspond to prime ideals of A which are contained in P. Hence the only maximal ideal of A_P corresponds to P. All other maximal ideals of A dissappear in A_P.

Definition. *Let P be a prime ideal of a ring A. The residue field of A at P is*

$$k(P) = A_P/M_P.$$

Example. $p\mathbb{Z}_{(p)}$ is the only maximal ideal of $\mathbb{Z}_{(p)}$. Note that $\mathbb{Z}_{(p)}$ isn't a field (p isn't invertible in $\mathbb{Z}_{(p)}$). The residue field of $\mathbb{Z}$ at (p) is

$$k((p)) = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p.$$

9.8. Definition. *A ring A is called a local ring if* $\text{m-Spec}\,(A)$ *consists of one element, i.e. A has exactly one maximal ideal.*

Examples. The localization A_P is a local ring.

Every field is a local ring.

9.9. Theorem. *Let A be an integral domain with field of fractions K. For every prime ideal P we have $A \subset A_P \subset K$. Then A is equal to the intersection of all A_M where M runs through all maximal ideals of A.*

Proof. Let $x \in K$. Consider the ideal I_x of denominators of x, i.e. $I_x = \{a \in A : ax \in A\}$. If $I_x \not\subset P$ then x can be written as a fraction b/c with $b, c \in A$ and $c \in A \setminus P$, hence $x \in A_P$. Conversely, if $x \in A_P$ then $I_x \not\subset P$.

If I_x is proper ideal of A then it is contained in a maximal ideal M, hence $x \notin A_M$. Thus, if x belongs to the intersection of all A_M, then $I_x = A$ and so $1 \in I_x$ and $x \in A$.

9.10. For an ideal I of a ring A and an A-module M denote by IM the A-submodule of M generated by im where $i \in I, m \in M$.

Nakayama's Lemma. *Let N be an A-module of finite type. Let I be an ideal of A.*

If $N = IN$ then there is an element $a \in 1 + I$ such that $aN = 0$.

Proof. Let $N = IN$. Assume that $N \neq 0$. Let $n_1, \dots, n_k \in N$ be generators of the A-module N. Then $n_1 \in N = IN$, so $n_1 = \sum_{j=1}^{k} b_{1j} n_j$ with $b_{1j} \in I$. Then $(1 - b_{11})n_1 - b_{12}n_2 - \dots - b_{1k}n_k = 0$. Similarly we find b_{ij} for $i = 2, \dots, n$. Denote $C = E - B$, where $B = (b_{ij})$. Then the product of the matrix C and the column consisting of $n_1, \dots, n_k$ equals the zero column. Multiplying C by its adjugate matrix we obtain $\det(C)N = 0$. Finally, $a = \det(C) \in 1 + I$.

If N is a torsion free A-modules and $I \neq A$ then $a \in 1 + I$ implies $a \neq 0$ and so $aN = 0$ implies $N = 0$.

The following property holds over local rings for any finitely generated modules.

Corollary 1. *Let M be the maximal ideal of a local ring A and let N be an A-module of finite type. Suppose that $MN = N$. Then $N = 0$.*

Proof. By Nakayama's Lemma there is an element $a \in 1 + M$ such that $aN = 0$.

If A is a local ring and M is its maximal ideal, then $1 + M \subset A^{\times}$. Indeed, if for some $m \in M$ the element $1 + m$ were not a unit of A, then the ideal $(1+m)$ would be a proper ideal of A, hence it would be contained

in the maximal ideal M; since $m \in M$ we would get $1 = 1+m-m \in M$, a contradiction.

Since $1 + M \subset A^\times$, there is $b \in A$ such that $ba = 1$. Now $N = baN = 0$.

Corollary 2. *Let N be an A-module of finite type. Let $f: N \to N$ be a homomorphism of A-modules. Then f is an isomorphism iff f is surjective.*

Proof. Define on the abelian group N the structure of $A[X]$-module by indicating the action of X on N:

$$X \cdot n := f(n), \quad n \in N$$

and extending it to the action of $A[X]$, i.e. $(\sum a_i X^i) \cdot n = \sum a_i X^i \cdot n$, and $X^i \cdot n = (f \circ \cdots \circ f)(n)$, where the composite of f with itself is taken i times.

Let $I = XA[X]$. Then $f(N) = N$ implies $IN = N$.

By Nakayama's Lemma we know that there is an element $a \in 1 + I$ such that $aN = 0$. The element a can be written as $1 + p(X)X$ for a polynomial $p(X) \in A[X]$. Then for every n in the kernel of f we have

$$0 = an = (1+p(X)X)n = n+p(X)\cdot(X\cdot n) = n+p(X)\cdot(f(n)) = n+0 = n.$$

Thus, f is injective.

9.11. Let A be an integral domain. Let M be an A-module. Let S be a multiplicative subset of A. Define the module of fractions M_S of M with respect to S as the equivalence classes of m/s, $m \in M$, $s \in S$ with respect to the equivalence relation $m/s \sim m'/s'$ iff $s'm - m's = 0$, with the natural addition and multiplication by elements of A_S. Thus, M_S is an A_S-module.

If N is a submodule of M, then N_S can be viewed as a submodule of M_S. The homomorphism of A_S-modules $M_S \to (M/N)_S$, $m/s \mapsto$

$(m+N)/s$, is surjective and its kernel is the image of N_S: if $(m+N)/s \sim (0+N)/s'$ then $s'(m+N) = 0+N$, hence $s'm \in N$ and $m/s \simeq s'm/(s's)$ belongs to the image of N_S.

Thus,

$$(M/N)_S \simeq M_S/N_S.$$

9.12. If $S = A \setminus P$ for a prime ideal P of A, then we write $M_P = M_S$ and call it the localization of M with respect to P.

Lemma. $A_S \otimes_A M \simeq M_S$, $f: (a/s, m) \mapsto am/s$.

Proof. The map is A-bilinear, so we obtain $A_S \otimes_A M \to M_S$. Define a map $M_S \to A_S \otimes_A M$, $m/s \to 1/s \otimes m$. This is well defined: if $sm' = s'm$ then

$$1/s \otimes m = s'/(ss') \otimes m = 1/(ss') \otimes s'm = 1/(ss') \otimes sm' = 1/s' \otimes m'.$$

This map is the inverse to f.

10. Completion

10.1. Definition. Let I be an ideal of a ring A. Consider the set of sequences (a_n), $n \geqslant 1$, of elements of A, such that $a_n - a_m \in I^m$ for all $n \geqslant m \geqslant 1$. Consider equivalence classes with respect to the following equivalence relation: $(a_n) \sim (b_n)$ if $a_n - b_n \in I^n$ for all $n \geqslant 1$. Introduce the ring structure on the equivalence classes via $(a_n) + (b_n) = (a_n + b_n)$, $(a_n)(b_n) = (a_n b_n)$. This ring is denoted $\widehat{A}$ and is called the completion of A with respect to the ideal I.

We have a ring homomorphism $\phi: A \to \widehat{A}$, $a \mapsto (a)$. The completion $\widehat{A}$ is an A-module via ϕ. The kernel of ϕ is equal to $\cap I^n$.

If ϕ is an isomorphism then A is called a completed ring.

For every n we have a surjective ring homomorphism $\psi_n\colon \widehat{A} \to A/I^n$, in fact already $\psi_n(\phi(A)) = A/I^n$.

The completion $\widehat{A}$ is also denoted as $\varprojlim A/I^n$.

10.2. Examples. 1. Let $A = B[X]$. Let $I = XB[X]$. Then $\varprojlim A/I^n$ is isomorphic to the ring $B[[X]] = \{\sum_{i\geqslant 0} b_i X^i : b_i \in B\}$ with the natural operations of addition and multiplication. To prove this, use representatives of cosets of A modulo I^n by polynomials of degree $< n$. Then, for two polynomials p_n, p_m of degree $n-1$ and $m-1$, $n \geqslant m \geqslant 1$, such that $p_n + I^m = p_m + I^m$ we deduce that the monomials of degree $\leqslant m-1$ of p_n are equal to the monomials of degree $\leqslant m-1$ of p_m. Now, to a sequence (a_n) such that $a_n + I^m = a_m + I^m$ for $n \geqslant m \geqslant 1$ associate the power series $\sum_{i\geqslant 0} c_i X^i$, $c_i \in B$, such that the polynomial $p_n = \sum_{0\leqslant i\leqslant n-1} c_i X^i$ is the representative of the coset $a_n + I^n$. In this example, ϕ is injective, but not surjective.

2. Let $A = \mathbb{Z}$ and $I = a\mathbb{Z}$ for $a > 1$. Then $\varprojlim A/I^n$ is isomorphic to the ring of a-adic numbers $\mathbb{Z}_a = \sum_{n\geqslant 0} c_n a^n$, $c_n \in \{0, 1, \ldots, a-1\}$. In this example, ϕ is injective, but not surjective. In particular, if a is a positive prime number p, the corresponding ring $\mathbb{Z}_p$ of p-adic integers is one of central objects in number theory. The product of all $\mathbb{Z}_p$ where p ranges through all positive primes, is called the profinite completion of $\mathbb{Z}$ and is denoted $\widehat{\mathbb{Z}}$.

3. More generally, we can similarly define the completion $\varprojlim A/I_n$ of a ring A with respect to a decreasing sequence of its ideals I_n which are not necessarily powers I^n of one fixed ideal.

Lemma. *(1) Let M be a maximal ideal of a ring A. Then $\widehat{M} = \{(a_n) \in \widehat{A} : a_1 \in M\}$ is a maximal ideal of $\widehat{A}$. The ring $\widehat{A}$ is a local ring.*

(2) The completion $\widehat{A_M} = \varprojlim A_M/(MA_M)^i$ of the localization A_M with respect to its ideal MA_M is isomorphic to the completion $\widehat{A} = \varprojlim A/M^i$ of A with respect to M via the homomorphism $(a_n) \mapsto (a_n/1)$.

Proof. (1) The kernel of the surjective ring homomorphism $\psi_1\colon \widehat{A} \to A/M$ is exactly $\widehat{M}$, hence $\widehat{A}/\widehat{M}$ is a field.

If $(a_n) \in \widehat{A} \setminus \widehat{M}$, then $a_1 \notin M$ and since $a_i + M = a_1 + M$ we deduce $a_i \notin M$. Then $M + a_iA \neq M$, so $a_iA + M = A$ and $A \subset a_iA + (a_iA + M)M \subset a_iA + M^2$, and similarly $A = a_iA + M^i$ for every i. Thus, $a_i + M^i$ is invertible in A/M^i. Let $b_i \in A$ be such that $(b_i+M^i)(a_i+M^i) = 1+M^i$. Then $(b_n) \in \widehat{A}$: indeed, $b_n \equiv b_{n+1}a_{n+1}b_n \equiv b_{n+1}a_nb_n \equiv b_{n+1} \mod M^n$. We get $(a_n)(b_n) = 1$ in $\widehat{A}$, so $(a_n) \in \widehat{A}^\times$. We conclude that every element of $\widehat{A} \setminus \widehat{M}$ is a unit of $\widehat{A}$, hence $\widehat{M}$ is the only maximal ideal of $\widehat{A}$.

(2) The homomorphism from A/M^i to A_M/M^iA_M, given by $a + M^i \mapsto a/1+M^iA_M$, is an isomorphism: it is injective, since if $a/1 = m/s$ with $m \in M^i$, $s \in A\setminus M$, then $as \in M^i$, but $a-ast \in M^i$ where $t+M^i$ is the inverse of $s+M^i$, so $a \in M^i$; it is surjective, since for s, t as above we get $a - ast \in M^i$ for every $a \in A$ and hence $a/s - ta/1 \in M^iA_M$, so a/s is the image of $ta \in A$.

Thus, $M^nA_M \cap A = M^n$ and $A + M^nA_M = A_M$.

Let $(a_n) \in \widehat{A}$ and assume that $(a_n/1) = 0$ in $\widehat{A_M}$. Then $a_n \in M^nA_M \cap A = M^n$, so $(a_n) = 0$ in $\widehat{A}$. Let $(b_n) \in \widehat{A_M}$, find $a_n \in A$ such that $a_n - b_n \in M^nA_M$ which exist by the previous paragraph. Then $a_n - a_m - (b_n - b_m) \in M^mA_M$ and $b_n - b_m \in M^mA_M$ for $n \geqslant m \geqslant 1$, so $a_n - a_m \in M^mA_M \cap A = M^m$ and $(a_n) \in \widehat{A}$ and then the image of (a_n) is (b_n). Thus, the homomorphism from the completion $\widehat{A}$ of A with respect to M to the completion $\widehat{A_M}$ of A_M with respect to MA_M, $(a_n) \mapsto (a_n/1)$, is an isomorphism.

10.3. Definition. Similarly, for an A-module R define $\widehat{R} = \varprojlim R/I^nR$, as a set it consists of equivalence classes of sequences (r_n), $n \geqslant 1$, of elements of R, such that $r_n - r_k \in I^kR$ for all $n \geqslant k \geqslant 1$, with respect to the following equivalence relation: $(r_n) \sim (r'_n)$ if $r_n - r'_n \in I^nR$ for all $n \geqslant 1$.

Define the A-module structure of $\widehat{M}$ by $(r_n) + (r'_n) = (r_n + r'_n)$ and $a(r_n) = (ar_n)$. We can also view $\widehat{R}$ as an $\widehat{A}$-module via $(a_n)(r_n) = (a_n r_n)$.

More generally, we can define the completion $\varprojlim R/R_n$ is an A-module R with respect to a decreasing sequence of its submodules R_n.

We have the following properties of the completions which show up the flexibility with respect to the ideals or submodules involved in their definitions.

Fix l and consider sequences (r_n) of elements of R, such that $r_n - r_k \in I^{k+l}R$ for all $n \geqslant k \geqslant 1$, with the equivalence relation $(r_n) \sim (r'_n)$ if $r_n - r'_n \in I^{n+l}R$ for all $n \geqslant 1$. Then $\varprojlim R/I^{n+l}R \simeq \varprojlim R/I^n R$, $(r_n) \mapsto (s_n)$, where $s_n = r_{n-l}$ for $n \geqslant l$ and s_j for $j < l$ is such that $s_j + I^j R = s_l + I^j R$.

More generally, if we have two decreasing sequences of ideals I_n and J_n of A such that there is l so that $I_{n+l} \subset J_n$ for all n and there is s so that $J_{n+s} \subset I_n$ for all n, then $\varprojlim A/I_n = \varprojlim A/J_n$.

Similarly for A-modules, if we have two decreasing sequences of submodules R_n and R'_n of an A-module R such that there is l so that $R_{n+l} \subset R'_n$ for all n and there is s so that $R'_{n+s} \subset R_n$ for all n, then $\varprojlim R/R_n = \varprojlim R/R'_n$.

10.4. Let N be an A-submodule of M. Then $I^n(M/N) = (I^n M + N)/N$, so the A-module homomorphism $M/I^n M \to (M/N)/(I^n(M/N)) \simeq M/(I^n M + N)$ is surjective and its kernel is $(I^n M + N)/I^n M$ which is isomorphic to $N/I^n M \cap N$.

Theorem (Artin–Rees). *Let A be a Noetherian ring. Let M be an A-module of finite type. Let I be an ideal of A and let N be an A-submodule of M. Then there is r such that for all $n \geqslant r$*

$$I(N \cap I^n M) = N \cap I^{n+1} M.$$

Proof. The ideal I has finitely many generators, say, $x_1, \ldots, x_m$. Define an action of the polynomial ring $A[X_1, \ldots, X_m]$ on

$$M^* = \oplus_{n \geqslant 0} I^n M = M \oplus IM \oplus I^2 M \oplus I^3 M \oplus \ldots,$$

where X_i acts on an element of the module $I^n M$ as multiplication by x_i, sending it to an element of the module $I^{n+1} M$.

If $m_1, \ldots, m_s$ are generators of the A-module M, then it is easy to check that the elements of M^*: $m_1' = (m_1, 0, 0, ...)$, ..., $m_s' = (m_s, 0, 0, \ldots)$ are generators of the $A[X_1, \ldots, X_m]$-module M^*.

Define $N^* = \oplus_{n \geqslant 0} N \cap I^n M = N \oplus (N \cap IM) \oplus (N \cap I^2 M) \oplus \ldots$. This is a subset of M^* and is an $A[X_1, \ldots, X_m]$-submodule, since $I(N \cap I^n M) \subset N \cap I^{n+1} M$.

The ring $A[X_1, \ldots, X_m]$ is Noetherian by Theorem 4.7 and the module M^* is a Noetherian $A[X_1, \ldots, X_m]$-module by Corollary 3 of 4.6.

For $k \geqslant 1$ define

$$N_k = N \oplus (N \cap IM) \oplus \cdots \oplus (N \cap I^k M) \oplus I(N \cap I^k M) \oplus I^2 (N \cap I^k M) \oplus \ldots$$

Then $N_0 \subset N_1 \subset N_2 \subset \ldots$ is an increasing sequence of $A[X_1, \ldots, X_m]$-submodules of M^*. Thus, it stabilizes and its union N^* equals to N_r for some $r \geqslant 0$. This means $I(N \cap I^n M) = N \cap I^{n+1} M$ for all $n \geqslant r$, as required.

10.5. Corollary 1. *We have* $I^{k+r} N \subset N \cap I^{k+r} M \subset I^k N$, $k \geqslant 0$, *hence*

$$\widehat{N} = \varprojlim N/I^n N \simeq \varprojlim N/N \cap I^n M.$$

The map $\widehat{N} \to \widehat{M}$ *is injective, so we can view* $\widehat{N}$ *as a submodule of* $\widehat{M}$. *Then* $\widehat{M}/\widehat{N}$ *is isomorphic to* $\widehat{M/N} = \varprojlim (M/N)/(I^n (M/N))$.

Proof of Corollary. The previous theorem implies $I(N \cap I^r M) = N \cap I^{r+1} M$, and similarly, $I^k (N \cap I^r M) = N \cap I^{r+k} M$. Using the last paragraph of 10.3 we obtain $\widehat{N} = \varprojlim N/N \cap I^n M$.

The kernel of $\widehat{N} \to \widehat{M}$ consists of equivalence classes of sequences (a_n), $a_n \in N$, such that $a_n \in I^n M$, hence $a_n \in N \cap I^n M$ and so the equivalence class of (a_n) in $\widehat{N} = \varprojlim N/N \cap I^n M$ is zero.

If the image of an element (b_n) representing an element of $\widehat{M}$ is zero in $\widehat{M/N} = \varprojlim M/(I^n M + N)$, then $b_n \in I^n M + N$ for all n, so we can write $b_n = c_n + d_n$ with $c_n \in I^n M$ and $d_n \in N$. Then the equivalence class of $(b_n) \in \widehat{M}$ is the same as the equivalence class of (d_n) in $\widehat{M}$, and $(d_n) \in \widehat{N}$. On the other hand, every element of $\widehat{N}$ is zero in $\widehat{M/N}$.

Finally, an element (e_m), $e_m \in M$, representing an element of $\widehat{M/N} = \varprojlim M/(N+I^n M)$, satisfies $e_m+N+I^l M = e_l+N+I^l M$ for $m \geqslant l \geqslant 1$, so there are elements $n_m \in N$ such that $e_m+n_m+I^l M = e_l+n_l+N+I^l M$ for $m \geqslant l \geqslant 1$. Then $(e_m + n_m)$ belongs to $\widehat{M}$ and its image in $\widehat{M/N}$ coincides with (e_m).

10.6. Corollary 2. *The homomorphism* $\widehat{A} \otimes_A M \to \widehat{M}$, $(a_n) \otimes m \mapsto (a_n m)$, *is an isomorphism of* $\widehat{A}$*-modules.*

Proof. The module M is finitely generated, write it as F/N where F is a free A-module of rank n, and N is its submodule. Thus we have homomorphisms $N \to F \to M$ which induce homomorphisms $\widehat{A} \otimes_A N \to \widehat{A} \otimes_A F \to \widehat{A} \otimes_A M$. Consider the following diagram of homomorphisms

$$\begin{array}{ccccc} \widehat{A} \otimes_A N & \longrightarrow & \widehat{A} \otimes_A F & \xrightarrow{f} & \widehat{A} \otimes_A M \\ {\scriptstyle h}\downarrow & & \downarrow & & {\scriptstyle g}\downarrow \\ \widehat{N} & \longrightarrow & \widehat{F} & \longrightarrow & \widehat{M} \end{array}$$

The homomorphism $\widehat{A} \otimes_A F \to \widehat{F}$ is an isomorphism, since $\widehat{A} \otimes_A F \simeq \widehat{A} \otimes_A A^n \simeq \widehat{A}^n = \widehat{A^n}$.

The module $\widehat{M} \simeq \widehat{F/N}$ is isomorphic to $\widehat{F}/\widehat{N}$ be the previous corollary. The composite $\widehat{A} \otimes_A F \to \widehat{F} \to \widehat{M}$ is the composite of an isomorphism and a surjective map, and it coincides with the composite of

$f\colon \widehat{A} \otimes_A F \to \widehat{A} \otimes_A M$ and $g\colon \widehat{A} \otimes_A M \to \widehat{M}$, hence the latter is surjective.

Since N is a finitely generated A-module as a submodule of the Noetherian A-module F (Corollary 3 of 4.6), we similarly obtain that $h\colon \widehat{A} \otimes_A N \to \widehat{N}$ is surjective.

Now if x belongs to the kernel of g, write it as $f(y)$ for an appropriate y (note that f is surjective since $F \to M$ is). Then the image of y in $\widehat{F}$ goes to zero in $\widehat{M}$, hence it comes from an element $z \in \widehat{N}$. Write $z = h(w)$ with $w \in \widehat{A} \otimes_A N$. Then the image of w with respect to $\widehat{A} \otimes_A N \to \widehat{A} \otimes_A F \to \widehat{F}$ coincides with the image of y, and hence y equals the image of w with respect to $\widehat{A} \otimes_A N \to \widehat{A} \otimes_A F$. This implies that x, the image of y, is zero. Thus g is an isomorphism, as required.

11. Projective and injective modules

Definition. *We call a sequence $N \to M \to K$ of A-modules and A-module homomorphisms exact at M if the image of N in M coincides with the kernel of $M \to K$. A general sequence is called exact if it is exact at each internal term.*

For example, a sequence

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

is exact if $N \to M$ is injective, the image of N in M coincides with the kernel of $M \to K$ and $M \to K$ is surjective. If we view N as a submodule of M then M/N is isomorphic to K.

11.1. Projective modules.

Definition. *A module P is called a (direct) summand of a module Q if there are homomorphisms $\pi\colon Q \to P$ and $i\colon P \to Q$ such that $\pi \circ i = \mathrm{id}_P$.*

Then i is injective and π is surjective.

Examples.

1. P is a summand of P, just take i and π as the identity morphisms. More generally, each of two isomorphic modules is a summand of each other.

2. Define $i\colon P \to P \oplus R, \pi\colon P \oplus R \to P$ by $i(p) = (p, 0), \pi(p, r) = p$. Then P is a summand of $P \oplus R$. Note that $i \circ \pi$ is not the identity map of $P \oplus R$.

3. Let P_k be a summand of Q_k, $k = 1, 2$. Then $P_1 \oplus P_2$ is a summand of $Q_1 \oplus Q_2$, just take $\pi = (\pi_1, \pi_2)$ and $i = (i_1, i_2)$.

Definition. *An exact sequence*

$$0 \longrightarrow R \xrightarrow{u} Q \xrightarrow{v} S \longrightarrow 0$$

splits if there is a homomorphism $w\colon S \to Q$ *such that* $v \circ w = \mathrm{id}_S$.

Lemma. *There is a split sequence*

$$0 \longrightarrow R \xrightarrow{u} Q \xrightarrow{v} S \longrightarrow 0$$

if and only if S *is a summand of* Q.

Proof. If the sequence splits then S is a summand of Q. Conversely, if S is a summand of Q, then put $R = \ker \pi$, so the sequence

$$0 \longrightarrow R \longrightarrow Q \xrightarrow{\pi} S \longrightarrow 0,$$

splits: $\pi \circ i = \mathrm{id}_S$.

Lemma. *The following are equivalent:*

(1) S *is a summand of* Q,

(2) Q *is isomorphic to* $S \oplus R$ *for a module* R,

Proof. (2) implies (1). (1) implies (2): let R be the kernel of $\pi\colon Q \to S$. Define a morphism $\rho\colon R \oplus S \to Q$ by $\rho((r, s)) = r + i(s)$. If $\rho((r, s)) = 0$,

then $0 = \pi(\rho((r,s))) = s$ and then $r = 0$. Hence ρ is a injective. Since $\pi(q - i\pi(q)) = \pi(q) - \pi(q) = 0$, $q - i\pi(q) = r$ for some $r \in R$. Then $q = \rho((r, \pi(q)))$. Therefore, ρ an isomorphism and Q is isomorphic to the direct sum of R and S.

Definition. *An A-module P is called projective if it is a summand of a free A-module.*

Examples.

1. Every free object is a summand of itself, therefore every free object is projective.

2. Let $A = \mathbb{Z}/6\mathbb{Z}$. By the Chinese remainder theorem A is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, so $\mathbb{Z}/2\mathbb{Z} \simeq 3\mathbb{Z}/6\mathbb{Z}$ is a projective $\mathbb{Z}/6\mathbb{Z}$-module. However, it is not a free $\mathbb{Z}/6\mathbb{Z}$-module, since every finite free $\mathbb{Z}/6\mathbb{Z}$-module has cardinality divisible by 6.

3. (without proof) Projective modules over PID are free. Projective modules over local rings are free.

11.2. Another characterization of projective modules.

Lemma. *The direct sum $P_1 \oplus P_2$ is projective if and only if P_1, P_2 are projective.*

Proof. Let $p_{P_k}: P_1 \oplus P_2 \to P_k$, $i_{P_k}: P_k \to P_1 \oplus P_2$, $k = 1, 2$, be morphisms introduced in example 2 above. If $P_1 \oplus P_2$ is a summand of a free object F with morphisms i, π, then P_k is a summand of F with morphisms $\pi_{P_k} \circ \pi$ and $i \circ i_{P_k}$.

If P_1, P_2 are summands of F_1, F_2, then by example 3) above $P_1 \oplus P_2$ is a summand of $F_1 \oplus F_2$ which is free by 2.6

Proposition. *An A-module P is projective iff for every two A-modules R, Q, a homomorphism $\beta: P \to Q$ and a surjective homomorphism $\alpha: R \to$*

Q

$$\begin{array}{ccccc} & & P & & \\ & & \beta\downarrow & & \\ R & \xrightarrow{\alpha} & Q & \longrightarrow & 0 \end{array}$$

there is a homomorphism $\gamma\colon P \to R$ *such that* $\beta = \alpha \circ \gamma$.

Proof. First assume that P is a free module with generators $p_i, i \in I$. Denote $q_i = \beta(p_i)$. Since α is surjective, $q_i = \alpha(r_i)$ for some $r_i \in R$. Define $\gamma\colon P \to R$ such that $\gamma(p_i) = r_i$ for all $i \in I$ and γ is an A-module homomorphism. Then $\alpha \circ \gamma(p_i) = \beta(p_i)$ and so $\alpha \circ \gamma = \beta$.

Now let P be projective, so there is a free module F and morphisms $\pi\colon F \to P$ and $i\colon P \to F$ such that $\pi \circ i = \mathrm{id}_P$. Then we get a morphism $\beta' = \beta \circ \pi\colon F \to Q$ and from the first paragraph we deduce that there is a morphism $\gamma'\colon F \to R$ such that $\alpha \circ \gamma' = \beta'$. Then for $\gamma = \gamma' \circ i\colon P \to R$ we get $\alpha \circ \gamma = \beta' \circ i = \beta \circ \pi \circ i = \beta$, so P satisfied the property of the proposition.

Conversely, assume P satisfies the property of the proposition. By 2.6 we can find a free module F such that P is its quotient, so we get a surjective homomorphism $\alpha\colon F \to P$. Using $\beta = \mathrm{id}_P\colon P \to P$ we obtain that there is a morhism $\gamma\colon P \to F$ such that $\alpha \circ \gamma = \mathrm{id}_P$. Thus, P is a summand of F and projective.

Corollary 1. *Let* P *be projective. Then for every three modules* S, R, Q *and a diagramme*

$$\begin{array}{ccccc} & & P & & \\ & & \beta\downarrow & & \\ S & \xrightarrow{\delta} & R & \xrightarrow{\alpha} & Q \end{array}$$

with the exact row and $\alpha \circ \beta = 0$ *there is a morphism* $\varepsilon\colon P \to S$ *such that*

$$\beta = \delta \circ \varepsilon.$$

Proof. Since $\alpha\circ\beta = 0$, we deduce that $\mathrm{im}(\beta) \subset \ker(\alpha) = \delta(S)$. Consider the epimorphism $\delta'\colon S \to \delta(S)$. From the proposition we deduce that there is a morphism $\varepsilon\colon P \to S$ such that $\beta = \delta' \circ \varepsilon$. Then $\beta = \delta \circ \varepsilon$.

Corollary 2. *P is projective iff every exact sequence*

$$0 \longrightarrow R \longrightarrow Q \xrightarrow{v} P \longrightarrow 0$$

splits.

Proof. If P is projective, then using $\beta = \mathrm{id}_P\colon P \to P$ the proposition implies there is $\gamma\colon P \to Q$ such that $v \circ \gamma = \mathrm{id}_P$, so the sequence splits.

By 2.6 there is an exact sequence

$$0 \longrightarrow R \longrightarrow F \xrightarrow{v} P \longrightarrow 0$$

with free F. Then it splits, so P is a summand of F, and therefore P is projective.

Example 3. Let $A = \mathbb{Z}/4\mathbb{Z}$. The sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

(the morphism $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is defined as $n + 4\mathbb{Z} \to n + 2\mathbb{Z}$) doesn't split, because otherwise $\mathbb{Z}/4\mathbb{Z}$ were isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and wouldn't be cyclic order 4. Thus, $\mathbb{Z}/2\mathbb{Z}$ isn't a projective $\mathbb{Z}/4\mathbb{Z}$-module.

11.3. Exactness of Hom and projective modules.

Definition. *A covariant functor $\mathcal{F}$ on A-modules is a map from the set of all A-modules to itself, and from all A-modules homomorphisms to itself, such that for every A-module homomorphism $f\colon M \to N$ we get an A-module homomorphism $\mathcal{F}(f)\colon \mathcal{F}(M) \to \mathcal{F}(N)$ and $\mathcal{F}(f \circ g) = \mathcal{F}(f) \circ \mathcal{F}(g)$, $\mathcal{F}(\mathrm{id}_M) = \mathrm{id}_{\mathcal{F}(M)}$.*

A contravariant functor $\mathcal{F}$ on A-modules is a map from the set of all A-modules to itself, and from all A-modules homomorphisms to itself,

such that for every A*-module homomorphism* $f\colon M \to N$ *we get an* A*-module homomorphism* $\mathcal{F}(f)\colon \mathcal{F}(N) \to \mathcal{F}(M)$ *and* $\mathcal{F}(f \circ g) = \mathcal{F}(g) \circ \mathcal{F}(f)$, $\mathcal{F}(\mathrm{id}_M) = \mathrm{id}_{\mathcal{F}(M)}$.

Examples of functors.

1. The covariant functor $\mathcal{H}om(T, \cdot)$, $U \mapsto \mathrm{Hom}(T, U)$, $f\colon M \to N$ is mapped to
$\mathcal{H}om(f)\colon \mathrm{Hom}(T, M) \to \mathrm{Hom}(T, N)$, $g \mapsto f \circ g$.

2. The contravariant functor $\mathcal{H}om(\cdot, T)$, $U \mapsto \mathrm{Hom}(U, T)$, $f\colon M \to N$ is mapped to $\mathcal{H}om(f)\colon \mathrm{Hom}(N, T) \to \mathrm{Hom}(M, T)$, $g \mapsto g \circ f$.

3. The covariant functor $\otimes_A T$, $U \mapsto U \otimes_A T$, $f\colon M \to N$ is mapped to
$\otimes_A T(f)\colon M \otimes_A T \to N \otimes_A T$, $m \otimes t \mapsto f(m) \otimes t$.

Definition. *A covariant functor* $\mathcal{F}$ *is called exact (left exact, right exact) if for every short exact sequence*

$$0 \longrightarrow R \longrightarrow Q \longrightarrow S \longrightarrow 0$$

the sequence

$$0 \longrightarrow \mathcal{F}(R) \longrightarrow \mathcal{F}(Q) \longrightarrow \mathcal{F}(S) \longrightarrow 0$$

is exact (exact everywhere with exception of $\mathcal{F}(S)$*, exact everywhere with exception of* $\mathcal{F}(R)$*).*

Lemma. *The functor* $\mathcal{H}om(T, \cdot)$ *is left exact.*

Proof. Let

$$0 \to R \xrightarrow{u} Q \xrightarrow{v} S \longrightarrow 0$$

be an exact sequence. If $f\colon T \to R$ and $u \circ f\colon T \to Q$ is the zero morphism, then $f(T) = 0$ and so f is the zero morphism.

For $f\colon T \to R$ clearly $v \circ u \circ f\colon T \to S$ is the zero morphism. If $g\colon T \to Q$ is such that $v \circ g\colon T \to S$ is the zero morphism, then for every

$t \in T$ $g(t) = u(r_t)$ for a uniquely determined $r_t \in R$. Define $f: T \to R$ by $f(t) = r_t$. It is a morphism and $g = u \circ f$.

Similarly one can show that the contravariant functor $\mathcal{H}om(\cdot, T): \mathcal{Q} \to \mathcal{Q}$ is left exact, i.e. for an exact sequence

$$0 \longrightarrow R \longrightarrow Q \longrightarrow S \longrightarrow 0$$

the sequence

$$0 \longrightarrow \mathrm{Hom}(S, T) \longrightarrow \mathrm{Hom}(Q, T) \longrightarrow \mathrm{Hom}(R, T)$$

is exact.

Exercise. *Show that the functor $\otimes_A T$ is right exact.*

Corollary 3. *P is projective iff the functor $\mathcal{H}om(P, \cdot): \mathcal{Q} \to \mathcal{Q}$ is exact.*

Proof. Let P be projective. Let

$$0 \longrightarrow R \longrightarrow Q \xrightarrow{v} S \longrightarrow 0$$

be an exact sequence. For every morphism $g: P \to S$ there is a morphism $f: P \to Q$ such that $g = v \circ f$. Thus, the morphism $\mathrm{Hom}(P, Q) \to \mathrm{Hom}(P, S)$ is surjective.

Let the functor $\mathcal{H}om(P, \cdot)$ be exact. Then for every epimorphism $v: Q \to S$ and a morphism $g: P \to S$ there is a morphism $f: P \to Q$ such that $g = v \circ f$. Hence by the propostion P is projective.

11.4. Injective objects.

Definition. *An A-module J is called injective if for every two A-modules R, Q, an A-module homomorphism $\beta: R \to J$ and an injective A-module homomorphism $\alpha: R \to Q$*

$$\begin{array}{ccc} 0 & \longrightarrow & R \\ & & \downarrow{\scriptstyle \beta} \\ & & J \end{array} \qquad \begin{array}{c} \xrightarrow{\alpha} \\ \\ \\ \end{array} \qquad \begin{array}{c} Q \\ \\ \\ \end{array}$$

there is a morphism $\gamma\colon Q \to J$ *such that*

$$\beta = \gamma \circ \alpha.$$

Note that there is no characterization of injective objects in terms of free objects.

Properties of injective objects.

1. The finite direct sum of modules is injective iff each object is injective.

2. If J is injective, then for every three modules S, R, Q and a diagramme

$$\begin{array}{ccccc} Q & \xrightarrow{\delta} & R & \xrightarrow{\alpha} & S \\ & & \downarrow{\scriptstyle \beta} & & \\ & & J & & \end{array}$$

with exact row and $\beta \circ \delta = 0$ there is a morphism $\varepsilon\colon S \to J$ such that $\beta = \varepsilon \circ \alpha$.

3. J is injective iff the functor $\mathcal{H}om(\cdot, J)$ is exact.

4. J is injective $\Rightarrow$ every exact sequence

$$0 \longrightarrow J \longrightarrow Q \longrightarrow R \longrightarrow 0$$

splits.

Remark. For every module Q there is an injective module J and a monomorphism $Q \to J$. The proof is a little tricky and is omitted.

Using this result one can replace $\Rightarrow$ in 4 by $\Leftrightarrow$.

Definition. *An* A*-module* Q *is called divisible if for every* $q \in Q$ *and* $a \in A$ *which is not a zero divisor there is* $q' \in Q$ *such that* $q = aq'$. *For example,* $\mathbb{Q}$ *is a divisible* $\mathbb{Z}$*-module.*

One can prove that

1. $\mathbb{Z}$-module Q is injective iff Q is divisible.

2. If Q is an A-module, then the A-module $\mathrm{Hom}_{\mathbb{Z}}(A, Q)$ is a divisible A-module.