Algebra 2 2004/2005

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 $f: A \to B$ 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 $g: A/I \to C$, $a+I \mapsto f(a)$. 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:*

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

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

For an ideal J of A, $I \subset J$, denote by $h|_J: J \to A/I, j \mapsto j + I$ the restriction of h to J. Its kernel is I and so by the previous theorem its image is isomorphic to J/I. The latter 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

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

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) *(they are called improper ideals of* A*).*

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 $adf = bcf = edf$, $d(af - be) = 0$. 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 $J_1 = I_1, J_2 = I_2 \ldots I_n$, so $J_1 J_2 = I_1 \ldots I_n$. Since $I_1 + I_k = A$ for all $k > 1$, we deduce using 1.2 that

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

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,

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

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

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

2. Modules over rings

2.1. 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. A map $f: M \to N$ 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. 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.

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 $f: N \oplus K \to N+K$, $f((n,k)) = n+k$ is a surjective A-module homomorpism whose kernel is in one-to-one correspondence with the set $N \cap K$. 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. 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.

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

M is said to be of *finite type* if it has a finite number of generators. Every module of finite type has finite rank.

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.

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 every element of M is annihilated by multiplication by n.

3. Polylinear constructions

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

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

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

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

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

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 out of $f(m_i, n_j)$. 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 $\mathrm{Bil}_A(M, N; R) \simeq \mathrm{Hom}_A(T, R)$.

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

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

(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.

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

These satisfy the 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 $M \otimes N$ and is called the *tensor product of M and N over A*. In particular, we have $n \otimes 0 = 0(n \otimes 1) = 0$.

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

3.4. Theorem. *For an A-bilinear map $f\colon M \times N \to R$ define $f'\colon M \otimes_A N \to R$ 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 $L \to R$ by $l_{m,n} \mapsto f(m, n)$. Since f is bilinear, all generators of K are mapped to zero, so we get $f' = \alpha(f)\colon M \otimes N \to R$, $f'(\sum a_i m_i \otimes n_i) = \sum a_i f(m_i, n_i)$. The map α is a homomorphism of A-modules.

Conversely, if $f'\colon M \otimes N \to R$ is a homomorphism of A-modules, then define $f = \beta(f')\colon M \times N \to R$ 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 $\beta \circ \alpha(f)(m, n) = f(m, n)$.

Thus, α and β are isomorphisms.

So 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 lemma the vector space of linear maps $M \otimes N \to F$ 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 $f\colon M \times N \to F$ is determined by its values on $\{(m_i, n_j)\}$.

Therefore, the dimension of the vector space $\mathrm{Hom}_F(M \otimes N, F)$ 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 $M \otimes N$ is $d_1 d_2$; the F-vector space $M \otimes N$ 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 $N \otimes N$ 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 $N \otimes N$ 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 $l_{m,n} \mapsto l_{n,m}$ 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 $f\colon m \otimes n \mapsto mn$. 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. The module $M^\circ = \mathrm{Hom}_A(M, A)$ is called the *A-dual module* to M.

We have a bilinear pairing $M \times M^\circ \to A$, $(m, f) \mapsto f(m)$ which induces a homomorphism $M \otimes_A M^\circ \to A$ and a homomorphism $M \to M^{\circ\circ}$. For vector spaces over a field it is injective and by counting the dimensions of the spaces one can show that the latter homomorphism is an isomorphism.

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.

We have a homomorphism

$$M^\circ \otimes_A N^\circ \to (M \otimes_A N)^\circ, \quad f \otimes g \mapsto (m \otimes n \mapsto f(m)g(n)).$$

In the case of vector spaces it is an isomorphism.

As a corollary of 3.5, (iv) 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, counting dimensions, we deduce that the homomorphism $M^\circ \otimes_A N^\circ \to (M \otimes_A N)^\circ \to \mathrm{Hom}_A(M, N^\circ)$ is an isomorphism, which gives a new definition of the tensor product of vector spaces: $M \otimes_A N = \mathrm{Hom}_A(M^\circ, N)$.

In the case where $N = M^\circ$ we conclude that $M^\circ \otimes_A M$ is isomorphic 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 $M_m = M_{m+1} = \ldots$;

$(ii) \Rightarrow (iii)$: 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 an 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 $E = N$.

4.2. Definition. A ring A is called *Noetherian* if A is a Noetherian A-module. In other words the conditions of 5.1 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 corresponence 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

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

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 $a = p_1a_1$ 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 $(p_1) \ldots (p_n) = (q_1) \ldots (q_m)$. 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 $q_1 \ldots q_m \in (p_1)$ 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 $p_2 \ldots p_n$ is equal to $q_2 \ldots q_m$, and hence $(p_2) \ldots (p_n) = (q_2) \ldots (q_m)$. 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 $\mathbb{Z}$: $\pm 2, \pm 3, \pm 5, \ldots$; 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 $a = up_1^{n_1} \ldots p_r^{n_r}$ and $b = vp_1^{m_1} \ldots p_r^{m_r}$ with units u, v, prime p_i and non-zero m_i, n_i, then $d = wp_1^{l_1} \ldots p_r^{l_r}$ 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 there is no prime element of A which divides all the coefficients of f.

Lemma. *Every polynomial 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 f.*

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 $a = d/e$.

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

Proof. Let p be a prime element of A. Let $f(X) = a_nX^n + \cdots + a_0$ and $g(X) = b_mX^m + \cdots + b_0$. 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 of X^{r+s} of fg is $a_rb_s + \sum_{i<r} a_ib_{r+s-i} + \sum_{j<s} a_{r+s-j}b_j$. Since a_i for $i < r$ and b_j for $j < s$ are divisible by p, p doesn't divide c.

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 polynomial f in $A[X]$ 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 the previous lemma. 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 $A[X]$.

Let f be a non-zero polynomial in $A[X]$. Write $f = ag$ with some non-zero $a \in A$ and a primitive polynomial g. The latter can be factorized in $K[X]$ as $\prod g_i$ with irreducible polynomials $g_i \in K[X]$. In accordance with 6.2 let $a_i \in K^\times$ be such that $a_i g_i$ is a primitive polynomial. 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 $A[X]$. Thus, all the prime elements of $A[X]$ are 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.

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 such that $F = A/pA$ is a field. Let $f(X) \in A[X]$ be a 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 primitive 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. Hence $\overline{f} = \overline{g}\overline{h}$ 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 $(2n+1)X^2 + (2l+1)X + (2k+1)$ is irreducible in $\mathbb{Z}[X]$ for all integer n, l, k.

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

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

$n > 0$. 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 of positive degree 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 $\mathbb{Z}$.

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 $y_1, \ldots, y_k$ are A-linearly expressible via elements $x_1, \ldots, x_k$, but $x_1, \ldots, x_k$ are A-linearly expressible via elements $y_1, \ldots, y_k$.

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 $x_1, \ldots, x_n$ such that $a_1x_1, \ldots, a_kx_k$ 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 $x_1, \ldots, x_n$ be a basis of M. Let $y_1, \ldots, y_m$ be generators of N. Each of them can be written as a linear combination of x_i with coefficients in A:

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

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

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

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

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 $x_1, \ldots, x_n$ such that N is generated by $a_1x_1, \ldots, a_kx_k$. 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, $a_1x_1, \ldots, a_kx_k$ 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 $a_1 \ldots a_i$, we deduce that

$$d_i(C) = a_1 \ldots a_iu = a_id_{i-1}(C)v$$

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*

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

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

Proof. Let $r_1, \ldots, r_n$ 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 $I_i = a_iA$. So the sequence of the ideals $I_1, \ldots, I_n$ 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 $M_i = A/p^mA$ 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 $I \neq 0$.

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 principal prime ideals (a) where a runs through all classes of prime elements of A up to multiplication by a unit of A and zero.

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 $f\colon A \to B$ 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

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

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

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:

$$V\colon \text{ideals of } \mathbb{C}[X_1, \ldots, X_n] \to \text{algebraic varieties of } \mathbb{C}^n,$$
$$J\colon \text{subsets } X \text{ of } \mathbb{C}^n \to \text{ideals of } \mathbb{C}[X_1, \ldots, X_n].$$

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 $V(J(V(I)) = V(I)$. Hence the maps V and J are 1-1 correspondences between

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

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 $y \not/ x$ there is a polynomial f such that $f(x) = 0 \neq f(y)$ we deduce $V(M_x) = \{x\}$. 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, $\mathrm{m-Spec}((\mathbb{C}[X_1, \ldots, X_n]) = \{M_x\}$ 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.

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 $J(V)$. It is easy to see that maximal ideals of $\mathbb{C}[V]$ correspond to maximal ideal 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. 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) A is an integral domain, $S = A \setminus \{0\}$. Then $S^{-1}A$ is 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. For example,

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

3) Geometric interpretation of the localization.

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

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

9.4. Define a homomorphism

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

The kernel of ϕ is equal to $\{a \in A : \text{ there is } s \in S \text{ such that } as = 0\}$. If A is an integral domain then ϕ is injective. It isn't injective in general, for example, $A = \mathbb{Z}[X]/(2X)$, $S = S_2$, $\phi(X + (2X)) = 0$.

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

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 $(p - s)u = 0$ for some $u \in S$. Then $su = pu \in P$ which contradicts $su \in S$.

If $a/s \cdot b/t = p/u$ with $p \in P$, $u \in S$, then $(abu - pst)v = 0$ and $(ab)(uv) = pstv \in P$. Since $uv \in S$ 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 $\alpha\colon P \mapsto S^{-1}P$ for $P \cap S = \emptyset$ and $\beta\colon Q \mapsto \phi^{-1}(Q)$ 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 there is $u \in S$ such that $u(p - as) = 0$, i.e. $a(us) \in P$. Since $us \in S$, we have $us \notin P$. Since P is prime 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,* Spec $(A_P) = \{QA_P : Q \in \text{Spec}\,(A), Q \subset P\}$, 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 m-Spec (A) consists of one element, i.e. A has exactly one maximal ideal.

Example. The localization A_P is a local ring. Every field is a local ring.

9.9. If A is a local ring and M is its maximal ideal, then $1 + M \subset A^\times$. Indeed, if for some $m \in M$ $1 + m$ were not a unit of A, then the ideal $(1 + m)$ is a proper ideal of A, hence it is contained in the maximal ideal M; since $m \in M$ we would get $1 = 1 + m - m \in M$, a contradiction.

9.10. Nakayama's Lemma. *Let N be a module over a ring A generated by k elements $n_1, \ldots, n_k$. Let I be an ideal of A.*

a) If $N = IN = \{\sum_{j=1}^{k} c_j n_j : c_j \in I\}$ then there is an element $a \in 1 + I$ such that $aN = 0$.

b) If M is the maximal ideal of a local ring A and $MN = N$, then $N = 0$.

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

b) If M is the maximal ideal of a local ring A, then every element of $1 + M$ is a unit, so the conditions of (a) are satisfied. So there is an element $a \in 1 + M$ such that $aN = 0$. Since $1 + M \subset A^\times$, there is $b \in A$ such that $ba = 1$. Now $N = baN = 0$.

Corollary. *Let A be a commutative ring with unity and 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:

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

Let $I = XA[X]$. Then $f(N) = N$ implies $IN = N$ and by part (a) of 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.