CHAPTER 0: PRELIMINARIES

§1: RINGS

(0.1) Definition: A ring R is a nonempty set together with two binary operations, "+" and "·", such that:

(a) R is an abelian group with respect to "+".

(b) R is a semigroup with respect to "·".

(c) The distributive laws hold: For all $a,b,c \in R$:

$$a(b+c) = ab+ac \quad \text{and} \quad (b+c)a = ba+ca.$$

Note that a semigroup is a nonempty set with an associative operation.

Throughout the course we only study commutative rings R with an identity element 1_R, i.e. $(R,\cdot)$ is a commutative semigroup with an identity element $1_R = 1$. In the following a ring R is a commutative ring with identity element. Note that we allow the case where $1=0$, that is, R may be the null ring.

(0.2) Definition: Let R and S be rings, i.e. R and S are commutative rings with identity elements 1_R and 1_S, respectively. A map $\varphi: R \longrightarrow S$ is called a homomorphism of rings if

(a) For all $a,b \in R$: $\varphi(a+b) = \varphi(a)+\varphi(b)$

(b) For all $a,b \in R$: $\varphi(ab) = \varphi(a)\varphi(b)$

(c) $\varphi(1_R) = 1_S$.

(0.3) Definition: Let R be a ring.

(a) A subset $S \subseteq R$ is called a subring of R if S is closed under subtraction and multiplication and if $1_R \in S$.

(b) A subset $I \subseteq R$ is called an ideal of R if

(i) I is an additive subgroup of R

(ii) For all $a \in I$ and all $r \in R$: $ar \in I$.

Ideals are much more interesting than subrings! The reason is that if $I \subseteq R$ is an ideal then we can define the quotient ring R/I. The structure of R/I relates to the structure of R and is in many cases simpler. There is another reason related to algebraic geometry. The set of equations satisfied by the points of an algebraic variety is an ideal in the polynomial ring over a field.

(0.4) Remark: Let $\varphi: R \longrightarrow S$ be a homomorphism of rings, $I \subseteq S$ an ideal. Then:

(a) $\varphi^{-1}(I) \subseteq R$ is an ideal called the contraction of I.

(b) If $J \subseteq R$ is an ideal its image $\varphi(J)$ is not an ideal of S unless φ is surjective. The smallest ideal of S containing $\varphi(J)$ is called the extension of J to S.

(c) $\varphi(R) \subseteq S$ is a subring of S.

(0.5) Remark: Let $\varphi: R \longrightarrow S$ and $\psi: S \longrightarrow T$ be homomorphisms of rings. The composition $\psi\varphi: R \longrightarrow T$ is a homomorphism of rings.

(0.6) Remark: Let R be a ring, $I \subseteq R$ an ideal. In particular, $(R,+)$ is an abelian group and I is a normal subgroup of R. The quotient group R/I is an abelian group under the operation $(a+I)+(b+I) = (a+b)+I$ for all $a,b \in R$. R/I is a commutative ring with identity $1_{R/I} = 1+I$ under the multiplication $(a+I)(b+I) = ab+I$ for all $a,b \in R$. The natural map $\nu: R \longrightarrow R/I$ defined by $\nu(a) = a+I$ is a surjective homomorphism of rings.

(0.7) Remark: Let R be a ring and $I \subseteq R$ an ideal. The maps:

$$\Phi: \{J \mid J \subseteq R \text{ an ideal with } I \subseteq J\} \longrightarrow \{K \mid K \subseteq R/I \text{ an ideal}\}$$

$$J \longrightarrow \nu(J) = \Phi(J)$$

$\Psi: \{K \mid K \subseteq R/I \text{ an ideal}\} \longrightarrow \{J \mid J \subseteq R \text{ an ideal with } I \subseteq J\}$

$$K \longmapsto \nu^{-1}(K) = \Psi(K)$$

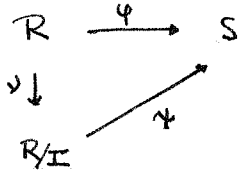
are inverse to each other and order preserving, that is, $J_1 \subseteq J_2 \Rightarrow \Phi(J_1) \subseteq \Phi(J_2)$ and $K_1 \subseteq K_2 \Rightarrow \Psi(K_1) \subseteq \Psi(K_2)$. Conclusion: There is a one-to-one order preserving correspondence between the ideals of R which contain I and the ideals of R/I.

(0.8) Definition: Let $\varphi: R \longrightarrow S$ be a homomorphism of rings. The kernel of φ, $\ker\varphi$, is defined by: $\ker\varphi = \varphi^{-1}(0) = \{a \in R \mid \varphi(a) = 0\}$.

(0.9) Remark: (a) $\ker\varphi$ is an ideal of R.

(b) $\ker\varphi = 0 \iff \varphi$ is injective.

(0.10) Theorem: Let $\varphi: R \longrightarrow S$ be a homomorphism of rings and $I \subseteq \ker\varphi$ an ideal of R. Then there is a unique homomorphism of rings $\psi: R/I \longrightarrow S$ so that the diagram



commutes, i.e. $\psi\nu = \varphi$, where $\nu: R \longrightarrow R/I$ is the natural map.

(0.11) Corollary: (First Isomorphism Theorem) Let $\varphi: R \longrightarrow S$ be a homomorphism of rings. φ induces an isomorphism of rings:

$$R/\ker\varphi \cong \varphi(R) \subseteq S$$

where $\varphi(R)$ is a subring of S.

(0.12) Definition: A ring $R \neq \{0\}$ is called an (integral) domain if whenever $a, b \in R$ with $ab = 0$ it holds that $a = 0$ or $b = 0$.

(0.13) Definition: Let R be a ring, $I, J, I_\lambda \subseteq R$, $\lambda \in \Lambda$, ideals of R.

(a) $I+J = \{a+b \mid a\in I \text{ and } b\in J\}$, the sum of the ideals I and J.

$\sum_{\lambda\in\Lambda} I_\lambda = \{\sum_{\lambda\in\Lambda} a_\lambda \mid a_\lambda\in I_\lambda \text{ and all, but finitely many } a_\lambda = 0\}$,
the sum of the ideals I_λ

$I\cdot J = \{\sum_{i=1}^{n} a_i b_i \mid n\in\mathbb{N}, a_i\in I, b_j\in J\}$, the product of the ideals I and J.

(b) Let $S\subseteq R$ be a subset. The ideal (S) generated by S is the smallest ideal of R that contains S:

$$(S) = \bigcap_{\substack{J\subseteq R \text{ an ideal}\\ S\subseteq J}} J$$

If $\{a_\lambda\}_{\lambda\in\Lambda}\subseteq I$, we say that I is generated by $\{a_\lambda\}_{\lambda\in\Lambda}$ if I is the smallest ideal which contains $\{a_\lambda\}_{\lambda\in\Lambda}$.

(c) An ideal $I\subseteq R$ is called principal if there is an $a\in I$ with $I=(a)=\{ar\mid r\in R\}$.

(d) R is called a principal ideal domain (PID) if R is a domain and every R-ideal is principal.

(0.14) Remark: Let R be a ring and $I, J, K\subseteq R$ ideals.

(a) If $I=(a_\lambda)_{\lambda\in\Lambda}$, that is, if I is generated by $\{a_\lambda\}_{\lambda\in\Lambda}$, then

$$I = (a_\lambda)_{\lambda\in\Lambda} = \{\sum_{\lambda\in\Lambda} b_\lambda a_\lambda \mid b_\lambda\in R \text{ and all, but finitely many } b_\lambda = 0\}.$$

(b) The operations "$+, \cdot, \cap$" on ideals are commutative and associative. Moreover, the distributive law holds: $I(J+K) = IJ + IK$.

(0.15) Definition: Let $R_1, \dots, R_n$ be rings. The direct product of $R_1, \dots, R_n$ is defined by:

$$R = \prod_{i=1}^{n} R_i = \{(a_1, \dots, a_n) \mid a_i\in R\}$$

R is a commutative ring with componentwise addition and multiplication and with identity element $1_R = (1, \dots, 1)$.

(0.16) Remark: Notation as in (0.15). For all $1\le j\le n$ there are natural maps:

$p_j : R \longrightarrow R_j$ defined by $p_j(a_1, \dots, a_n) = a_j$ and $i_j : R_j \longrightarrow R$ defined by $i_j(a) = (0, \dots, 0, a, 0, \dots, 0)$ where a is at the jth place. The <u>projection</u> map p_j is a surjective homomorphism of rings. The <u>embedding</u> is injective with the property: $i_j(a+b) = i_j(a) + i_j(b)$ and $i_j(ab) = i_j(a)\, i_j(b)$ for all $a, b \in R_j$. However, i_j is <u>not</u> a homomorphism of rings since the identity element $1 \in R_j$ is not mapped into the identity element of R (if $n \geq 2$ and at least 2 of the rings R_i are not the null ring).

(0.17) <u>Definition</u>: Let R be a ring and $S \subseteq R$ a subset. S is called a <u>multiplicative</u> subset of R if $1 \in S$ and for all $a, b \in S$ the element $ab \in S$ is in S.

(0.18) <u>Definition</u> and <u>Proposition</u>: Let R be a ring and $P \subseteq R$ an ideal. The following conditions are equivalent:

(a) R/P is an integral domain.

(b) $P \neq R$ and for all $a, b \in R$: $ab \in P \Rightarrow a \in P$ or $b \in P$

(c) $P \neq R$ and for all ideals $I, J \subseteq R$: $IJ \subseteq P \Rightarrow I \subseteq P$ or $J \subseteq P$.

(d) $R - P$ is a multiplicative subset of R.

An ideal $P \subseteq R$ which satisfies one of the above conditions is called a <u>prime ideal</u> of R.

<u>Proof</u>: (a) $\Rightarrow$ (b): R/P is an integral domain, thus $R/P \neq \{0\}$ and $P \neq R$. Let $a, b \in R$ with $a \cdot b \in P$. Then $ab + P = (a+P)(b+P) = 0 + P$ in R/P and hence $a \in P$ or $b \in P$.

(b) $\Rightarrow$ (c): Suppose $I \not\subseteq P$ and $J \not\subseteq P$ and let $a \in I - P$ and $b \in J - P$. Then $ab \notin P$ and thus $IJ \not\subseteq P$.

(c) $\Rightarrow$ (b): Set $I = (a)$ and $J = (b)$ and note that $ab \in P \Longleftrightarrow IJ \subseteq P$.

(b) $\Rightarrow$ (a): Let $a+P, b+P \in R/P$ with $(a+P)(b+P) = 0+P$. Thus $ab \in P$ and hence $a \in P$ or $b \in P$ implying $a + P = 0 + P$ or $b + P = 0 + P$.

(b) $\Longleftrightarrow$ (d): trivial

(0.19) Example: (a) Let R be a factorial domain (for example: $R=\mathbb{Z}$) and $p\in R$ a prime element. Then $(p)\subseteq R$ is a prime ideal. Moreover, a principal ideal $(a)\subseteq R$ is a prime ideal if and only if $a=0$ or a is a prime element of R.
(b) Let K be a field and x,y,z variables over K. The ideals (x,y), (y,z), $(x+1, y-2, z+3)$ are prime ideals of $R = K[x,y,z]$.

(0.20) Definition: Let R be a ring and $m\subseteq R$ an ideal with $m\neq R$. m is a maximal ideal of R if for every ideal $I\subseteq R$ with $m\subseteq I$ either $m=I$ or $I=R$.

(0.21) Proposition: Let R be a ring and $m\subseteq R$ an ideal. The following conditions are equivalent:
(a) R/m is a field.
(b) $m\subseteq R$ is a maximal ideal.

Proof: (a) $\Rightarrow$ (b): The only ideals of the field R/m are (0) and R/m. By (0.7) the only ideals of R containing m are m and R.
(b) $\Rightarrow$ (a): Let $a+m \in R/m$ with $a+m \neq 0+m$. Then $a\notin m$ and $m+(a)=R$. Hence there is a $t\in m$ and a $b\in R$ with $t+ab=1 \Rightarrow (a+m)(b+m)=1+m$.
R/m is a field.

§2: MODULES

(0.22) **Definition:** Let R be a ring. An R-module M is an abelian (additive) group $(M,+)$ together with a map $\varphi: R \times M \longrightarrow M$

$$(a,m) \longmapsto \varphi(a,m) = am$$

so that for all $a, a_i \in R$ and all $m, m_i \in M$:

(a) $a(m_1 + m_2) = am_1 + am_2$

(b) $(a_1 + a_2)m = a_1 m + a_2 m$

(c) $(a_1 a_2)m = a_1(a_2 m)$

(d) $1_R \cdot m = m$.

(0.23) **Remark:** Let $(M,+)$ be an abelian group and

$$\mathrm{End}(M) = \{\tau: M \longrightarrow M \mid \tau \text{ a homomorphism of groups}\}$$

the set of all endomorphisms of M. $\mathrm{End}(M)$ is a (noncommutative) ring under the operations $(\tau+\sigma)(m) = \tau(m) + \sigma(m)$ and $(\tau\sigma)(m) = \tau(\sigma(m))$ for all $m \in M$. M is an R-module if and only if there is a homomorphism of rings $\Phi: R \longrightarrow \mathrm{End}(M)$ with $\Phi(1_R) = \mathrm{id}_M$.

(0.24) **Definition:** Let M and N be R-modules.

(a) A map $\varphi: M \longrightarrow N$ is an R-*module homomorphism* or an R-*linear map* if

(i) For all $m, m' \in M$: $\varphi(m+m') = \varphi(m) + \varphi(m')$

(ii) For all $a \in R$, $m \in M$: $\varphi(am) = a\varphi(m)$.

(b) $\mathrm{Hom}_R(M,N) = \{\varphi: M \longrightarrow N \mid \varphi \ R\text{-linear}\}$ denotes the set of all R-linear maps from M to N.

(0.25) **Remark:** Let M, N, and L be R-modules.

(a) If $\varphi \in \mathrm{Hom}_R(M,N)$ and $\psi \in \mathrm{Hom}_R(N,L)$ then $\psi\varphi \in \mathrm{Hom}_R(M,L)$

(b) Define an addition and a scalar multiplication on $\mathrm{Hom}_R(M,N)$ by: for all

$m \in M$ and $a \in R$:

$(\varphi_1+\varphi_2)(m) = \varphi_1(m) + \varphi_2(m)$ and $(a\varphi_1)(m) = a\varphi_1(m)$.

Then $\varphi_1+\varphi_2$, $a\varphi_1 \in \mathrm{Hom}_R(M,N)$ and $\mathrm{Hom}_R(M,N)$ is an R-module.

(c) $\mathrm{Hom}_R(M,M)$ is a (noncommutative) ring under multiplication the composition of maps.

(0.26) Definition: Let M be an R-module.

(a) A subset $N \subseteq M$ is an R-submodule of M if

(i) N is a subgroup of $(M,+)$

(ii) For all $a \in R$ and all $n \in N$: $an \in N$.

(b) Let $N \subseteq M$ be an R-submodule. The factor group M/N is an R-module under the scalar multiplication: $a(m+N) = am + N$ for all $a \in R$, $m \in M$. M/N is called the factor or quotient module of M by N.

(0.27) Remark: Let R be a ring and M, N R-modules.

(a) R is naturally an R-module. The R-submodules of R are exactly the ideals of R.

(b) Let $L \subseteq M$ be an R-submodule. The natural map $\varphi: M \longrightarrow M/L$ defined by $\varphi(m) = m+L$ for all $m \in M$ is R-linear.

(c) Let $\varphi: M \longrightarrow N$ be an R-linear map. The kernel of φ: $\ker(\varphi) = \{m \in M \mid \varphi(m)=0\}$ is a submodule of M and the image of φ $\mathrm{im}(\varphi) = \varphi(M)$ is a submodule of N.

(d) The module $N/\mathrm{im}(\varphi) = \mathrm{coker}(\varphi)$ is called the cokernel of φ.

(e) Let $\varphi: M \longrightarrow N$ be an R-linear map. Then:

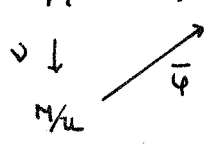
(i) φ is injective if and only if $\ker(\varphi) = 0$.

(ii) φ is surjective if and only if $\mathrm{im}(\varphi) = N \longleftrightarrow \mathrm{coker}(\varphi) = 0$.

(f) Let $N \subseteq M$ be a submodule. Then there is a 1-1 correspondence between the submodules $L \subseteq M$ with $N \subseteq L$ and the submodules of M/N.

$\{ L \subseteq M \mid L \text{ a submodule and } N \subseteq L \} \xleftrightarrow{\simeq} \{ \overline{L} \subseteq M/N \mid \overline{L} \text{ a submodule} \}$.

(0.28) Proposition: Let $\varphi: M \longrightarrow N$ be a linear map of R-modules and $U \subseteq M$ a submodule with $U \subseteq \ker(\varphi)$. There is exactly one R-linear map $\overline{\varphi}: M/U \longrightarrow N$ such that the diagram



commutes where ν is the natural map. Moreover, $\ker(\overline{\varphi}) = \ker(\varphi)/U$.

(0.29) Remark: (1^{st} Isomorphism Theorem) Assumptions as in (0.28). If $U = \ker(\varphi)$ then $\overline{\varphi}$ is injective and $M/\ker(\varphi) \cong U$.

(0.30) Examples: (a) Let $R = K$ be a field. The K-modules are exactly the K-vector spaces.

(b) Every abelian group $(M,+)$ is a $\mathbb{Z}$-module by: For all $n \in \mathbb{Z}$, $m \in M$:

$n=0$: $0m = 0$; $n>0$: $nm = \underbrace{m + \ldots + m}_{n\text{-times}}$; $n<0$: $nm = \underbrace{(-m) + \ldots + (-m)}_{(-n)\text{-times}}$

(c) Let R be a ring and I an index set. Consider the set:

$R^{(I)} = \{ f: I \longrightarrow R \mid f \text{ a map with } f(i) = 0 \text{ for all but finitely many } i \in I \}$

and define addition and scalar multiplication on $R^{(I)}$ by:

For all $f, g \in R^{(I)}$, $a \in R$, $i \in I$: $\quad (f+g)(i) = f(i) + g(i)$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (af)(i) = a f(i)$.

$R^{(I)}$ is an R-module under these operations. Modules of this form are called free R-modules. Usually the elements of $R^{(I)}$ are written as sequences $(a_i)_{i \in I} \in R^{(I)}$ where $a_i = 0$ for almost all $i \in I$. If I is a finite set with $|I| = n$ we write $R^{(I)} = R^n$.

(0.31) Remark: Let M be an R-module and $M_i \subseteq M$, $i \in I$, submodules of M.

(a) $\sum_{i \in I} M_i = \{ \sum_{i \in I} m_i \mid m_i \in M \text{ and } m_i = 0 \text{ for almost all } i \in I \}$

is a submodule of M called the sum of M_i, $i \in I$.

(b) $\bigcap_{i\in I} M_i$ is a submodule of M.

(c) $\sum_{i\in I} M_i = \bigcap_{\substack{N\subseteq M \text{ a submodule} \\ M_i\subseteq N\ \forall\, i\in I}} N$ that is, $\sum_{i\in I} M_i$ is the smallest submodule of M which contains M_i for all $i\in I$.

(0.32) Proposition: (More Isomorphism Theorems) Let M be an R-module and $M_1, M_2 \subseteq M$ submodules.

(a) If $M_2 \subseteq M_1$ then $(M/M_2)/(M_1/M_2) \cong M/M_1$

(b) $(M_1+M_2)/M_1 \cong M_2/(M_1\cap M_2)$.

Proof: (a) Define $\varphi: M/M_2 \longrightarrow M/M_1$ by $\varphi(m+M_2) = m+M_1$. φ is a well defined R-linear map with $\ker(\varphi) = M_1/M_2$. By the 1st Isomorphism Theorem (0.29): $(M/M_2)/(M_1/M_2) \cong \operatorname{im}(\varphi) = M/M_1$.

(b) Consider the map $\psi: M_2 \longrightarrow (M_1+M_2)/M_1$ defined by $\psi(m) = m+M_1$. ψ is a surjective R-linear map with $\ker(\psi) = M_1\cap M_2$. The statement follows again with (0.29).

(0.33) Definition: Let M be an R-module and $\{x_i\}_{i\in I} \subseteq M$.

(a) $\{x_i\}_{i\in I}$ is called a system of generators of M if $\sum_{i\in I} Rx_i = M$.

(b) $\{x_i\}_{i\in I}$ is called linearly independent if whenever $a_i, b_i \in R$ with $\sum'_{i\in I} a_i x_i = \sum'_{i\in I} b_i x_i$ then $a_i = b_i$ for all $i\in I$. ($\sum'_i$ indicates finite sums, i.e. $a_i = 0$ and $b_i = 0$ for all but finitely many $i\in I$).

(c) $\{x_i\}_{i\in I}$ is called a basis of M if $\{x_i\}_{i\in I}$ is a linearly independent system of generators of M.

(d) M is called a finite (or finitely generated) R-module if M has a finite system of generators.

(0.34) Remark: An R-module M is free $\Longleftrightarrow$ there is an index set I so that $M \cong R^{(I)}$ $\Longleftrightarrow$ M has a basis.

Let $\{M_i\}_{i\in I}$ be a family of R-modules. Set

$\bigoplus_{i\in I} M_i = \{ f: I \longrightarrow \dot{\bigcup}_{i\in I} M_i \mid f$ is a map with $f(i)\in M_i$ for all $i\in I$ and $f(i)=0$ for all but finitely many $i\in I\}$.

Usually we write the elements of $\bigoplus_{i\in I} M_i$ as 'sequences' $(m_i)_{i\in I}$ with $m_i\in M$ for all $i\in I$ and $m_i=0$ for almost all $i\in I$. Obviously $(m_i)_{i\in I}$ represents the map $f: I \longrightarrow \dot{\bigcup} M_i$ with $f(i)=m_i$ for all $i\in I$.

$\bigoplus_{i\in I} M_i$ is an R-module under the operations:

$(m_i) + (n_i) = (m_i+n_i)$ and $a(m_i) = (am_i)$ for all $a\in R$.

$\bigoplus_{i\in I} M_i$ is called the <u>direct sum</u> of $\{M_i\}_{i\in I}$.

(0.35) <u>Remark</u>: If $M_i = R$ for all $i\in I$, then $\bigoplus_{i\in I} R = R^{(I)}$.

(0.36) <u>Proposition</u>: Let N be an R-module and $M_1, \dots, M_n \subseteq N$ submodules. Suppose:

(a) $\sum_{i=1}^{n} M_i = N$

(b) For all $2\le i\le n$: $M_i \cap (M_1 + \dots + M_{i-1}) = (0)$.

Then $N \cong \bigoplus_{i=1}^{n} M_i$.

<u>Proof</u>: By induction on n: $n=1$: trivial

$n-1 \Rightarrow n$: Consider the R-linear map $\varphi: \bigoplus_{i=1}^{n} M_i \longrightarrow N$ defined by $\varphi(m_1, \dots, m_n) = m_1 + \dots + m_n$. By (a) φ is surjective. Suppose $\varphi(m_1, \dots, m_n) = \sum_{i=1}^{n} m_i = 0$, then $m_n = -\sum_{i=1}^{n-1} m_i \in M_n \cap \sum_{i=1}^{n-1} M_i = 0$. Hence $m_n = 0$ and $\sum_{i=1}^{n-1} m_i = 0$. Apply the induction hypothesis to the submodule $N' = \sum_{i=1}^{n-1} M_i \subseteq N$. Since $N' \cong \bigoplus_{i=1}^{n-1} M_i$ we obtain that $m_i = 0$ for all $i = 1, \dots, n-1$. Thus φ is injective.

Let $\{M_i\}_{i\in I}$ be a family of R-modules. For all $i\in I$ there are R-linear maps

$\kappa_i: M_i \longrightarrow \bigoplus_{i\in I} M_i$ and $p_i: \bigoplus_{i\in I} M_i \longrightarrow M_i$

defined by $\kappa_i(m) = (m_j)$ where $m_j = 0$ if $i\neq j$ and $m_i = m$ and by $p_i(m_j) = m_i$. p_i is surjective and called the i^{th} <u>projection</u> onto M_i. κ_i is injective. We

consider M_i a submodule of $\oplus_{i\in I} M_i$ via κ_i. Note that $p_i \kappa_i = id_{M_i}$.

(0.37) Proposition: Let $\{M_i\}_{i\in I}$ be a family of R-modules and N an R-module.
(a) Suppose that for every $i\in I$ there is given an R-linear map $f_i: M_i \longrightarrow N$. Then there is exactly one R-linear map $f: \oplus_{i\in I} M_i \longrightarrow N$ with $f\kappa_i = f_i$ for all $i\in I$.
(b) Suppose for all $i\in I$ there is given an R-linear map $g_i: N \longrightarrow M_i$ such that for all $n\in N$ $g_i(n) = 0$ for all but finitely many $i\in I$. Then there is a unique R-linear map $g: N \longrightarrow \oplus_{i\in I} M_i$ with $p_i g = g_i$ for all $i\in I$.

Proof: Homework

§3: THE TENSOR PRODUCT

(0.38) **Definition**: Let R be a ring; M, N, and T R-modules. A map $\varphi: M \times N \longrightarrow T$ is called R-bilinear if

(a) For all $m \in M$ the map $\varphi_m: N \longrightarrow T$ defined by $\varphi_m(n) = \varphi(m,n)$ is R-linear.

(b) For all $n \in N$ the map $\eta_n: M \longrightarrow T$ defined by $\eta_n(m) = \varphi(m,n)$ is R-linear.

(0.39) **Definition**: Let M and N be R-modules. A tensor product of M and N over R is an R-module $M \otimes_R N$ together with an R-bilinear map $\tau: M \times N \longrightarrow M \otimes_R N$ such that for every R-bilinear map $\varphi: M \times N \longrightarrow T$ from $M \times N$ into some R-module T there is a unique R-linear map $\alpha: M \otimes_R N \longrightarrow T$ with $\alpha\tau = \varphi$, that is, the diagram

$$\begin{array}{ccc} M \times N & \xrightarrow{\tau} & M \otimes_R N \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\alpha} & \\ & T & \end{array}$$

commutes.

(0.40) **Proposition**: Let M and N be R-modules. If the tensor product of M and N over R exists it is unique up to isomorphism.

Proof: Let $(M \otimes_R N, \tau: M \times N \longrightarrow M \otimes_R N)$ and $(M \tilde{\otimes}_R N, \tilde{\tau}: M \times N \longrightarrow M \tilde{\otimes}_R N)$ be two tensor products with bilinear maps τ and $\tilde{\tau}$. Then there is exactly one R-linear map $\alpha: M \otimes_R N \longrightarrow M \tilde{\otimes}_R N$ with $\alpha\tau = \tilde{\tau}$ and exactly one R-linear map $\tilde{\alpha}: M \tilde{\otimes}_R N \longrightarrow M \otimes_R N$ with $\tilde{\alpha}\tilde{\tau} = \tau$. Thus $\tilde{\alpha}\alpha\tau = \tau$ and $\alpha\tilde{\alpha}\tilde{\tau} = \tilde{\tau}$ implying that the diagrams

$$\begin{array}{ccc} M \times N & \xrightarrow{\tau} & M \otimes_R N \\ {\scriptstyle\tau}\downarrow & \overset{\tilde{\alpha}\alpha}{\swarrow}\ \overset{id}{\nwarrow} & \\ M \otimes_R N & & \end{array} \qquad \text{and} \qquad \begin{array}{ccc} M \times N & \xrightarrow{\tilde{\tau}} & M \tilde{\otimes}_R N \\ {\scriptstyle\tilde{\tau}}\downarrow & \overset{\alpha\tilde{\alpha}}{\swarrow}\ \overset{id}{\nwarrow} & \\ M \tilde{\otimes}_R N & & \end{array}$$

commute. By uniqueness: $\tilde{\alpha}\alpha = id_{M \otimes_R N}$ and $\alpha\tilde{\alpha} = id_{M \tilde{\otimes}_R N}$.

(0.41) **Theorem**: If M and N are R-modules, the tensor product of M and N over R exists

Proof: Let $R^{(M\times N)}$ be the free R-module with basis $M\times N$ and let $U \subseteq R^{(M\times N)}$ be the submodule which is generated by all elements of the form:

$(m+m', n) - (m,n) - (m',n)$

$(m, n+n') - (m,n) - (m,n')$

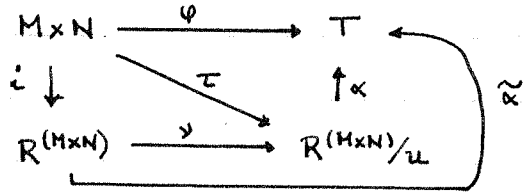
$(am, n) - a(m,n)$

$(m, an) - a(m,n)$ for all $m,m' \in M$, $n,n' \in N$, and $a \in R$.

Let τ be the composition of maps: $M\times N \xrightarrow{i} R^{(M\times N)} \xrightarrow{\nu} R^{(M\times N)}/U$ where i maps (m,n) into the basis element (m,n) of $R^{(M\times N)}$ and ν is the canonical map onto the quotient module.

Claim: $(R^{(M\times N)}/U, \tau)$ is the tensor product of M and N over R.

Pf of claim: Obviously, τ is R-bilinear. Let T be an R-module and $\varphi: M\times N \longrightarrow T$ an R-bilinear map. Considering φ as a map from the set $M\times N$ into the R-module T we can extend φ uniquely to an R-linear map $\tilde{\alpha}: R^{(M\times N)} \longrightarrow T$. Since φ is R-bilinear, $U \subseteq \ker(\tilde{\alpha})$, and there is a unique R-linear map $\alpha: R^{(M\times N)}/U \longrightarrow T$ such that the diagram:



commutes.

(0.42) Remark: (a) For elements $m \in M$ and $n \in N$ we set $m \otimes n = \tau(m,n)$.

(b) For all $m,m' \in M$; $n,n' \in N$; $a \in R$:

$$(m+m') \otimes n = m \otimes n + m' \otimes n$$

$$m \otimes (n+n') = m \otimes n + m \otimes n'$$

$$(am) \otimes n = m \otimes (an) = a(m \otimes n).$$

(c) Every element of $M \otimes N$ is of the form:

$$\sum_{i=1}^{r} a_i (m_i \otimes n_i) = \sum_{i=1}^{r} (a_i m_i) \otimes n_i = \sum_{i=1}^{r} m_i \otimes (a_i n_i)$$

where $m_i \in M$, $n_i \in N$, and $a_i \in R$.

(d) If $V = \{v_i\}_{i\in I}$ and $W = \{w_j\}_{j\in J}$ are generating sets of M and N, then $V \tilde{\otimes} W = \{v_i \otimes w_j\}_{i\in I, j\in J}$ is a generating set of $M \otimes_R N$.

(0.43) Example: $(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) = 0$

Proof: For all $q \in \mathbb{Q}/\mathbb{Z}$ there is an $n \in \mathbb{Z} - (0)$ with $nq = 0$ and for all $p \in \mathbb{Q}/\mathbb{Z}$, $m \in \mathbb{Z} - (0)$ there is a $p' \in \mathbb{Q}/\mathbb{Z}$ with $mp' = p$. For all $p, q \in \mathbb{Q}/\mathbb{Z}$ let $n \in \mathbb{Z} - (0)$ with $nq = 0$ and $p' \in \mathbb{Q}/\mathbb{Z}$ with $np' = p$. Then $q \otimes p = q \otimes (np') = (nq) \otimes p' = 0 \otimes p' = 0$.

Let $M_1, \dots, M_r$ be R-modules. Instead of starting with R-bilinear maps we can consider R-multilinear maps $\varphi: M_1 \times \cdots \times M_r \longrightarrow T$ (these are maps which are R-linear in every 'variable'). The proofs of (0.40) and (0.41) can be adjusted accordingly to show existence and uniqueness of the 'multi-tensor product' $M_1 \otimes \cdots \otimes M_r$. Note that $M_1 \otimes \cdots \otimes M_r$ is generated by all products $m_1 \otimes \cdots \otimes m_r$ where $m_i \in M_i$ for $1 \leq i \leq r$.

(0.44) Proposition: Let $M_1, \dots, M_r$ be R-modules. There exists a pair (T, τ) consisting of an R-module T and an R-multilinear map $\tau: M_1 \times \cdots \times M_r \longrightarrow T$ with the following property: For every R-module N and for every R-multilinear map $\varphi: M_1 \times \cdots \times M_r \longrightarrow N$ there is a unique R-linear map $\alpha: T \longrightarrow N$ such that $\alpha\tau = \varphi$. Moreover, if (T, τ) and (T', τ') are two pairs with this property, then there is a unique isomorphism $\psi: T \longrightarrow T'$ with $\psi\tau = \tau'$. T is denoted by $M_1 \otimes \cdots \otimes M_r$.

Proof: Homework

(0.45) Proposition: Let M, N, P be R-modules. Then there are unique isomorphisms:

(a) $M \otimes_R N \cong N \otimes_R M$ with $m \otimes n \longmapsto n \otimes m$

(b) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P) \cong M \otimes_R N \otimes_R P$ with $(m \otimes n) \otimes p \longmapsto m \otimes (n \otimes p) \longmapsto m \otimes n \otimes p$

(c) $R \otimes_R M \cong M$ with $a \otimes m \longmapsto am$.

Proof: Homework

(0.46) Proposition: Let M_i, $i \in I$, and N be R-modules. Then

$$\left(\oplus_{i\in I} M_i\right)\otimes_R N \cong \oplus_{i\in I}(M_i\otimes_R N)$$

Proof: The map $\varphi: (\oplus M_i)\times N \longrightarrow \oplus(M_i\otimes N)$ with $\varphi((m_i),n)=(m_i\otimes n)$ is R-bilinear. Thus there is an R-linear map $\alpha:(\oplus M_i)\otimes N \longrightarrow \oplus(M_i\otimes N)$ with $\alpha((m_i)\otimes n)=(m_i\otimes n)$. Conversely, for every $j\in I$ there is an R-bilinear map $\psi_j: M_j\times N \longrightarrow (\oplus M_i)\otimes N$ defined by $\psi_j(x,n)=(m_i)\otimes n$ where $m_i=0$ for $i\neq j$ and $m_j=x$. Thus for every $j\in I$ there is an R-linear map $\beta_j: M_j\otimes N \longrightarrow (\oplus M_i)\otimes N$ with $\beta_j(x\otimes n)=(m_i)\otimes n$ where $m_i=0$ for $i\neq j$ and $m_j=x$. By the universal property of the direct sum there is an R-linear map $\beta:\oplus(M_i\otimes N)\longrightarrow(\oplus M_i)\otimes N$ with $\beta((m_i\otimes n)_{i\in I})=(m_i)_{i\in I}\otimes n$. The maps α and β are inverse to each other on the generators. Thus $\alpha\beta=\mathrm{id}_{\oplus(M_i\otimes N)}$ and $\beta\alpha=\mathrm{id}_{(\oplus M_i)\otimes N}$.

(0.47) Definition: Let R and S be rings and P a nonempty set. P is called a (R,S)-bimodule if P is an R-module and a S-module and the two module structures are compatible in the following sense: for all $p\in P$, $a\in R$, $b\in S$: $a(pb)=(ap)b$.

(0.48) Proposition: Let R and S be rings, M an R-module, P an (R,S)-bimodule, and N a S-module. Then:

(a) $M\otimes_R P$ is naturally a S-module.

(b) $P\otimes_S N$ is naturally an R-module.

(c) $(M\otimes_R P)\otimes_S N \cong M\otimes_R(P\otimes_S N)$.

Proof: Homework.

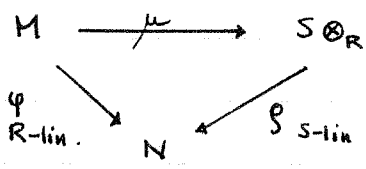
(0.49) Remark: Let $\varphi: R\longrightarrow S$ be a morphism of rings.

(a) If N is a S-module, N has an R-module structure by restriction of scalars: for all $a\in R$ and all $n\in N$ set $an=\varphi(a)n$. N is an (R,S)-bimodule.

(b) If M is an R-module consider the R-module ${}_SM = S\otimes_R M$. ${}_SM$ is a S-module via the following operation: For all $b,b'\in S$, $m\in M$ set $b(b'\otimes m)=(bb')\otimes m$. ${}_SM$ is obtained

from M by extension of scalars or by base change. ${}_SM$ has the following universal property:

(0,50) Proposition: For every S-module N and every R-linear map $\varphi: M \longrightarrow N$ there is a unique S-linear map $\varrho: {}_SM = S \otimes_R M \longrightarrow N$ with $\varphi = \varrho\mu$ where $\mu: M \longrightarrow S \otimes_R M$ is the R-linear map defined by $\mu(m) = 1 \otimes m$ for all $m \in M$.



(0,51) Remark and Definition: Let $\varphi: M' \longrightarrow M$ and $\psi: N' \longrightarrow N$ be R-linear maps of R-modules. The map $\beta: M' \times N' \longrightarrow M \otimes_R N$ defined by $\beta(m', n') = \varphi(m') \otimes \psi(n')$ is R-bilinear. Thus there is a unique R-linear map $\varphi \otimes \psi: M' \otimes_R N' \longrightarrow M \otimes_R N$ with $(\varphi \otimes \psi)(m' \otimes n') = \varphi(m') \otimes \psi(n')$. If $\varphi_2: M'' \longrightarrow M'$ and $\varphi_1: M' \longrightarrow M$ are R-linear maps and if N is an R-module then $(\varphi_1 \varphi_2) \otimes \mathrm{id}_N = (\varphi_1 \otimes \mathrm{id}_N)(\varphi_2 \otimes \mathrm{id}_N)$. Similarly, if $\psi_2: N'' \longrightarrow N'$ and $\psi_1: N' \longrightarrow N$ are R-linear maps and M is an R-module, then $\mathrm{id}_M \otimes (\psi_1 \psi_2) = (\mathrm{id}_M \otimes \psi_1)(\mathrm{id}_M \otimes \psi_2)$.

§4: CATEGORIES AND FUNCTORS

(0.52) **Definition**: A category $\mathcal{C}$ consists of

(1) a class of objects, denoted $\mathrm{obj}\,\mathcal{C}$

(2) pairwise disjoint sets of morphisms, denoted $\mathrm{Hom}_{\mathcal{C}}(A,B)$, for every ordered pair of objects (A,B)

(3) compositions $\mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A,C)$, denoted $(f,g) \longmapsto gf$, so that the following conditions are satisfied:

(a) for all $A \in \mathrm{obj}\,\mathcal{C}$ there exists an identity morphism $1_A \in \mathrm{Hom}_{\mathcal{C}}(A,A)$ such that $f 1_A = f$ for all $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ and $1_A g = g$ for all $g \in \mathrm{Hom}_{\mathcal{C}}(C,A)$ and all $B,C \in \mathrm{obj}\,\mathcal{C}$.

(b) associativity of composition holds whenever possible: if $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$, $g \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ and $h \in \mathrm{Hom}_{\mathcal{C}}(C,D)$, then $h(gf) = (hg)f$.

(0.53) **Remark**: (a) $\mathrm{Hom}_{\mathcal{C}}(A,B)$ is required to be a set. Note that $\mathrm{Hom}_{\mathcal{C}}(A,B)$ may be empty.

(b) For $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ we write $f: A \longrightarrow B$, although the elements of $\mathrm{Hom}_{\mathcal{C}}(A,B)$ may not be maps.

(c) The identity morphism $1_A \in \mathrm{Hom}_{\mathcal{C}}(A,A)$ is unique.

(0.54) **Examples**: (a) $\mathcal{C} \cong$ sets: The objects are sets, morphisms are functions, and the composition is the usual composition of functions.

(b) $\mathcal{C} \cong$ rings: Objects are rings, morphisms are homomorphisms of rings, composition is the usual composition of functions.

(c) $\mathcal{C} \cong$ groups: Objects are groups, morphisms are homomorphisms of groups, composition is the usual composition of functions.

(d) $\mathcal{C} \cong$ top: Objects are topological spaces, morphisms are continuous functions, composition is the usual composition of functions.

(e) $\mathcal{C} \cong \mathfrak{M}(R)$: R a commutative ring with identity, objects are R-modules, morphisms are R-linear maps, composition is the composition of functions.

(0.55) Definition: Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A covariant functor $F: \mathcal{C} \longrightarrow \mathcal{D}$ is a function satisfying:

(a) If $A \in \text{obj}\,\mathcal{C}$ then $FA \in \text{obj}\,\mathcal{D}$

(b) If $f: A \longrightarrow B$ is a morphism in $\mathcal{C}$ then $Ff: FA \longrightarrow FB$ is a morphism in $\mathcal{D}$.

(c) If $A \xrightarrow{f} B \xrightarrow{g} C$ are morphisms in $\mathcal{C}$, then $F(gf) = Fg\,Ff$.

(d) For every $A \in \text{obj}\,\mathcal{C}$: $F1_A = 1_{FA}$.

(0.56) Definition: Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A contravariant functor $F: \mathcal{C} \longrightarrow \mathcal{D}$ is a function satisfying:

(a) If $A \in \text{obj}\,\mathcal{C}$ then $FA \in \text{obj}\,\mathcal{D}$

(b) If $f: A \longrightarrow B$ is a morphism in $\mathcal{C}$ then $Ff: FB \longrightarrow FA$ is a morphism in $\mathcal{D}$.

(c) If $A \xrightarrow{f} B \xrightarrow{g} C$ are morphisms in $\mathcal{C}$, then $F(gf) = Ff\,Fg$.

(d) For every $A \in \text{obj}\,\mathcal{C}$: $F1_A = 1_{FA}$.

(0.57) Remark: The functors most relevant for this course are the two Hom-functors $\text{Hom}_R(M,-)$ and $\text{Hom}_R(-,N)$ and the tensor functors $M \otimes_R -$ and $- \otimes_R N$ (all from $\mathcal{M}(R)$ into itself).