

Kapitel III

Rings and modules

§ 11 Multilinear Algebra

In this section, R will always be a commutative, unitary ring.

Reminder 11.1 (i) An R -module is an abelian group $(M, +)$ together with a scalar multiplication

$$\cdot : R \times M \longrightarrow M$$

with the usual properties of a vector space, i.e. for any $m, n \in M, r, s \in R$ we have

$$(1) \quad r \cdot (s \cdot m) = (rs) \cdot m$$

$$(2) \quad (r + s) \cdot m = r \cdot m + s \cdot m$$

$$(3) \quad r \cdot (m + n) = r \cdot m + r \cdot n$$

$$(4) \quad 1_R \cdot m = m$$

(ii) A map $\phi : M \longrightarrow M'$ of R -modules M, M' is called R -linear or R -module homomorphism, if

$$\phi(r \cdot m + s \cdot n) = r \cdot \phi(m) + s \cdot \phi(n) \quad \text{for all } r, s \in R, m, n \in M.$$

(iii) A subset $S \subseteq M$ of an R -module is called an R -submodule of M , if S is an R -module.

(iv) R itself is an R -module, the submodules are the ideals of R .

(v) If $\phi : M \longrightarrow M'$ is R -linear, then

$$\ker(\phi) = \{m \in M \mid \phi(m) = 0\},$$

$$\operatorname{im}(\phi) = \{m' \in M' \mid \phi(m) = m' \text{ for some } m \in M\}$$

are R -submodules.

(vi) If $M \subseteq M'$ is a submodule, then the factor group M/M' is an R -module via

$$a \cdot \overline{m} = \overline{a \cdot m}.$$

(vii) For an R -linear map $\phi : M \longrightarrow M''$, we have

$$\text{im}(\phi) \cong M / \ker(\phi).$$

(viii) An R -module M is called *free*, if there exists a subset $X \subseteq M$, such that every $m \in M$ has a unique representation

$$m = \sum_{x \in X} a_x \cdot x, \quad a_x \in R, \quad a_x \neq 0 \text{ only for finitely many } x \in X.$$

In this case, X is called the rank of M .

(ix) Not every R -module is free: Indeed let $0 \subsetneq I \subsetneq R$ be a proper ideal. Then R/I is not free: Let $X \subseteq R$, such that $\overline{X} \subseteq R/I$ generates the R -module R/I . Let $x \in X$ and $a \in I \setminus \{0\}$. Then we have

$$x \cdot \overline{x} = \overline{a \cdot x} = \overline{0} = \overline{0 \cdot x} = 0 \cdot \overline{x},$$

hence we have found two different representations of 0. Thus R/I is not free.

(x) For any $n \in \mathbb{N}$, $n\mathbb{Z}$ is a free module

(xi) If $I \leq R$ is not a principal ideal, then I is not a free R -module., since for $x, y \in I$ with $y \notin (x)$ we have $xy - yx = 0$. Again we have a nontrivial representation of 0 and I is not free.

Definition + proposition 11.2 Let R be a ring, M, M' R -modules.

(i) The set of R -module homomorphisms

$$\text{Hom}_R(M, M') = \{\phi : M \longrightarrow M' \mid \phi \text{ is } R\text{-linear} \}$$

is again an R -module.

(ii) $M^* = \text{Hom}_R(M, R)$ is called the *dual module* of M .

Let now

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

be a short exact sequence of R -modules M, M', M'' , i.e. α is injective and β is surjective.

(iii) Then we have a short exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_R(N, M') & \xrightarrow{\alpha^*} & \text{Hom}_R(N, M) & \xrightarrow{\beta^*} & \text{Hom}_R(N, M'') \\ & & \phi & \mapsto & \alpha \circ \phi, & \psi & \mapsto & \beta \circ \psi \end{array}$$

(iv) We have a short exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_R(M'', N) & \xrightarrow{\beta^*} & \text{Hom}_R(M, N) & \xrightarrow{\alpha^*} & \text{Hom}_R(M', N) \\ & & \phi & \mapsto & \phi \circ \beta, & \psi & \mapsto & \psi \circ \alpha \end{array}$$

- (v) N is called a *projective* module, if β_* is surjective for all short exact sequences as in (iii).
 (vi) N is called an *injective* module, if α^* is surjective for all short exact sequences as in (iv).

proof. (i) This is clear: For all $\phi, \phi_1, \phi_2 \in \text{Hom}_R(M, M')$ and $a \in R$ we have

$$(\phi_1 + \phi_2)(x) = \phi_1(x) + \phi_2(x), \quad (a \cdot \phi)(x) = a \cdot \phi(x)$$

(iii) α_* is R -linear: For any $\phi_1, \phi_2 \in \text{Hom}_R(N, M')$ and $x \in N$ we have

$$\alpha_*(\phi_1 + \phi_2)(x) = (\alpha \circ (\phi_1 + \phi_2))(x) = \alpha(\phi_1(x) + \phi_2(x)) = \alpha(\phi_1(x)) + \alpha(\phi_2(x))$$

and thus

$$\alpha_*(\phi_1 + \phi_2)(x) = \alpha_*(\phi_1)(x) + \alpha_*(\phi_2)(x) = (\alpha_*(\phi_1) + \alpha_*(\phi_2))(x).$$

Moreover, α_* is injective: Since α is injective we have $\alpha_*(\phi)(x) = \alpha(\phi(x)) = 0$ if and only if $\phi(x) = 0$ for all $x \in N$, thus $\phi = 0$. Now we still have to show $\ker(\beta_*) = \text{im}(\alpha_*)$.

' \supseteq ' For $\phi \in \text{Hom}_R(N, M')$ we have $\beta_*(\alpha \circ \phi) = \beta \circ \alpha \circ \phi = 0 \circ \phi = 0$, i.e. $\alpha \circ \phi = \alpha_*(\phi) \in \ker(\beta_*)$.

' \subseteq ' Let $\phi : N \longrightarrow M$, $\phi \in \ker(\beta_*)$, i.e. $\beta \circ \phi = 0$. We have to show, that there exists $\phi' \in \text{Hom}_R(N, M')$ such that $\phi = \alpha_*(\phi') = \alpha \circ \phi'$. Let $x \in N$. Then $\phi(x) \in \ker(\beta) = \text{im}(\alpha)$. Then there exists $z \in M'$ such that $\phi(x) = \alpha(z)$ and z is unique, since α is injective. Define $\phi'(x) := z$. Then we have $\alpha \circ \phi' = \phi$. It remains to show that ϕ' is R -linear. We have $\phi'(x_1 + x_2) = z$ and with $\alpha(z) = \phi(x_1 + x_2) = \phi(x_1) + \phi(x_2)$ we again have $\alpha(z) = \phi(z_1) + \phi(z_2)$ for some suitable, but unique $z_1, z_2 \in M'$. Since we have

$$\alpha(z) = \phi(x_1 + x_2) = \phi(x_1) + \phi(x_2) = \alpha(z_1) + \alpha(z_2) = \alpha(z_1 + z_2)$$

and α is injective, we have $z = z_1 + z_2$, thus

$$\phi'(x_1 + x_2) = z = z_1 + z_2 = \phi'(x_1) + \phi'(x_2).$$

Moreover for $a \in R$ we have $\phi'(ax) = w$ with $\alpha(w) = \phi(ax) = a \cdot \phi(x) = a \cdot \alpha(z)$. Thus

$$\alpha(\phi'(ax)) = \alpha(w) = \phi(ax) = a \cdot \phi(x) = a \cdot \alpha(z) = a \cdot \alpha(\phi'(x)) \xrightarrow{\alpha \text{ inj.}} \phi'(ax) = a \cdot \phi'(x),$$

which proves the claim. \square

Remark 11.3 (i) An R -module N is projective if and only if for every surjective R -linear map $\beta : M \longrightarrow M''$ and every R -linear map $\phi : N \longrightarrow M''$ there is an R -linear map

$\tilde{\phi} : N \longrightarrow M$, such that the diagram below commutes, i.e. $\phi = \beta \circ \tilde{\phi}$.

$$\begin{array}{ccc} & & M \\ & \nearrow \tilde{\phi} & \downarrow \beta \\ N & \xrightarrow{\phi} & M'' \end{array}$$

(ii) Free modules are projective.

Definition 11.4 Let M, M_1, M_2 be R -modules. A map

$$\Phi : M_1 \times M_2 \longrightarrow M$$

is called *bilinear*, if the maps

$$\Phi_{x_0} : M_2 \longrightarrow M, \quad y \mapsto \Phi(x_0, y), \quad \Phi_{y_0} : M_1 \longrightarrow M, \quad x \mapsto \Phi(x, y_0)$$

are linear for all $x_0 \in M_1$ and $y_0 \in M_2$.

Definition 11.5 Let M_1, M_2 be R -modules. A *tensor product* of M_1 and M_2 is an R -module T together with a bilinear map

$$\tau : M_1 \times M_2 \longrightarrow T,$$

such that for every bilinear map $\Phi : M_1 \times M_2 \longrightarrow M$ for any R -module M there is a unique linear map $\phi : T \longrightarrow M$, such that the following diagram becomes commutative.

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\tau} & T \\ & \searrow \Phi & \swarrow \phi \\ & & M \end{array}$$

Remark 11.6 Let (T, τ) and (T', τ') be tensor products of R -modules M_1 and M_2 . Then there exists a unique isomorphism $h : T \longrightarrow T'$, such that

$$\tau' = h \circ \tau.$$

proof. Consider

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\tau} & T \\ & \searrow \tau' & \nearrow g \\ & & T' \end{array} \quad \begin{array}{c} \nearrow h \\ \searrow \end{array}$$

Existence and uniqueness of the linear maps g and h come from Definition 11.5. It remains to show, that $h \circ g = \text{id}_{T'}$ and $g \circ h = \text{id}_T$.

In order to do this, consider the following diagramm.

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\tau} & T \\ & \searrow \tau' & \swarrow g \circ h \stackrel{!}{=} \text{id}_T \\ & T & \end{array}$$

We have $(g \circ h)\tau = g \circ (h \circ \tau) = g \circ \tau' = \tau$. By the uniqueness we get $\text{id}_T = g \circ h$. Analogously we get $\text{id}_{T'} = h \circ g$ which finishes the proof. \square

Corollary 11.7 *The tensor product (T, τ) of R -modules M_1, M_2 is unique up to isomorphism. The standard notation is*

$$T = M_1 \otimes_R M_2, \quad \tau(x, y) = x \otimes y$$

Example 11.8 Let M_1, M_2 be free R -modules with bases $\{e_i\}_{i \in I}, \{f_j\}_{j \in J}$. Let T be the free R -module with basis $\{g_{ij}\}_{(i,j) \in I \times J}$ and

$$\tau : M_1 \times M_2 \longrightarrow T, \quad (e_i, f_j) \mapsto g_{ij} \quad \text{for all } (i, j) \in I \times J,$$

i.e. for elements in M_1, M_2 we have

$$\tau \left(\sum_{i \in I} a_i e_i, \sum_{j \in J} b_j f_j \right) = \sum_{(i,j) \in I \times J} a_i b_j g_{ij}$$

Then (T, τ) is the tensor product of M_1, M_2 , since: Let $\Phi : M_1 \times M_2 \longrightarrow M$ be bilinear. Define

$$\phi : T \longrightarrow M, \quad g_{ij} \mapsto \Phi(e_i, f_j).$$

Obviously ϕ is linear and satisfies $\Phi = \phi \circ \tau$. Now consider a special case and let $|I| = n, |J| = m$. Identify M_1 via (e_1, \dots, e_n) with R^n and M_2 via (f_1, \dots, f_m) with R^m . Then T is identified with $R^{n \times m}$ via

$$g_{ij} = E_{ij} = \begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ \vdots & & 1 & & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}$$

where the only nonzero entry is in the i -th row and j -th column. Then $\tau : R^n \times R^m \longrightarrow R^{n \times m}$ is given by

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} a_1 b_1 & \dots & a_1 b_m \\ \vdots & & \vdots \\ a_n b_1 & \dots & a_n b_m \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 & \dots & b_m \end{pmatrix},$$

where the last multiplication is the usual multiplication of matrices.

Theorem 11.9 *For any two R -modules M_1, M_2 there exists a tensor product $(T, \tau) = (M_1 \otimes_R M_2, \otimes)$.*

proof. Let F be the free R -module with basis $M_1 \times M_2$ and Q be the submodule generated by all the elements

$$(x + x', y) - (x, y) - (x', y), \quad (x, y + y') - (x, y) - (x, y'), \quad (ax, y) - a(x, y), \quad (x, ay) - a(x, y)$$

for $a \in R, x, x' \in M_1, y, y' \in M_2$. Define

$$T := F/Q, \quad \tau : M_1 \times M_2 \longrightarrow T, \quad (x, y) \mapsto \overline{(x, y)}.$$

Then by the construction of Q , τ is bilinear. Let now be M a further R -module and $\Phi : M_1 \times M_2 \longrightarrow M$ a bilinear map. Define

$$\tilde{\phi} : F \longrightarrow M, \quad (x, y) \mapsto \Phi(x, y).$$

Clearly $\tilde{\phi}$ is linear. Moreover we have $Q \subseteq \ker(\tilde{\phi})$, since Φ is bilinear. By the isomorphism theorem, $\tilde{\phi}$ factors to a linear map $\phi : T \longrightarrow M$ satisfying $\phi(\overline{(x, y)}) = \Phi(x, y)$. The uniqueness of ϕ follows by the fact that T is generated by the $\overline{(x, y)}$ for $x \in M_1, y \in M_2$. \square

Example 11.10 We want to find out what is

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}.$$

Let $\Phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \longrightarrow A$ bilinear for some \mathbb{Z} -module A . Then we see

$$\Phi(\bar{1}, \bar{1}) = \Phi(\bar{3}, \bar{1}) = \Phi(3 \cdot (\bar{1}, \bar{1})) = 3 \cdot \Phi(\bar{1}, \bar{1}) = \Phi(\bar{1}, \bar{3}) = \Phi(\bar{1}, \bar{0}) = 0 \cdot \Phi(\bar{1}, \bar{1}) = 0$$

Hence $\Phi = 0$, since $(\bar{1}, \bar{1})$ generates $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Thus $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$.

Proposition 11.11 *For R -modules M, M_1, M_2, M_3 we have the following properties.*

- (i) $M \otimes_R R \cong M$.
- (ii) $M_1 \otimes_R M_2 \cong M_2 \otimes_R M_1$.
- (iii) $(M_1 \otimes_R M_2) \otimes_R M_3 \cong M_1 \otimes_R (M_2 \otimes_R M_3)$.

proof. (i) Let $\tau : M \times R \longrightarrow M, (x, a) \mapsto a \cdot x$. Then τ is bilinear. We now can verify the universal property of the tensor product. Let N be an arbitrary R -module and $\Phi : M \times R \longrightarrow N$ be bilinear a bilinear map. Define

$$\phi : M \longrightarrow N, \quad x \mapsto \Phi(x, 1)$$

Then ϕ is R -linear: For $x, y \in M, \alpha \in R$ we have

$$\phi(\alpha \cdot x) = \Phi(\alpha \cdot x, 1) = \alpha \cdot \Phi(x, 1) = \alpha \cdot \phi(x),$$

$$\phi(x + y) = \Phi(x + y, 1) = \Phi(x, 1) + \Phi(y, 1) = \phi(x) + \phi(y)$$

and thus

$$\phi(\tau(x, a)) = \phi(a \cdot x) = a \cdot \Phi(x, 1) = \Phi(x, a)$$

(ii) The isomorphism

$$M_1 \times M_2 \xrightarrow{\cong} M_2 \times M_1, \quad (x, y) \mapsto (y, x)$$

induces an isomorphism $M_1 \otimes_R M_2 \cong M_2 \otimes_R M_1$.

(iii) For fixed $z \in M_3$ define

$$\Phi_z : M_1 \times M_2 \longrightarrow M_1 \otimes_R (M_2 \otimes_R M_3), \quad (x, y) \mapsto x \otimes (y \otimes z) = \tau_{1(23)}(\tau_{23}(x, y)).$$

Then Φ_z is bilinear and induces a linear map

$$\phi_z : M_1 \otimes_R M_2 \longrightarrow M_1 \otimes_R (M_2 \otimes_R M_3).$$

Define

$$\Psi : (M_1 \otimes_R M_2) \times M_3 \longrightarrow M_1 \otimes_R (M_2 \otimes_R M_3), \quad (x \otimes y, z) \mapsto \phi_z(x \otimes y).$$

Ψ is bilinear and induces a linear map

$$\psi : (M_1 \otimes_R M_2) \otimes_R M_3 \longrightarrow M_1 \otimes_R (M_2 \otimes_R M_3)$$

Doing this again the other way round we find a linear map

$$\tilde{\psi} : M_1 \otimes_R (M_2 \otimes_R M_3) \longrightarrow (M_1 \otimes_R M_2) \otimes_R M_3$$

By the uniqueness we obtain as in Remark 11.6 that $\psi \circ \tilde{\psi} = \tilde{\psi} \circ \psi = \text{id}$, hence the claim follows. \square

Definition + remark 11.12 Let M, M_1, \dots, M_n be R -modules.

(i) A map

$$\Phi : M_1 \times \dots \times M_n = \prod_{i=1}^n M_i \longrightarrow M$$

is called *multilinear*, if for any $1 \leq i \leq n$ and all choices of $x_j \in M_j$ for $j \neq i$ the map

$$\Phi_i : M_i \longrightarrow M, \quad x \mapsto \Phi(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n)$$

is linear.

(ii) The map

$$\tau_{M_1, \dots, M_n} : \prod_{i=1}^n M_i \longrightarrow \bigotimes_{i=1}^n M_i, \quad (x_1, \dots, x_n) \mapsto x_1 \otimes \dots \otimes x_n$$

is multilinear.

(iii) For every multilinear map

$$\Phi : \prod_{i=1}^n M_i \longrightarrow M$$

there exists a unique linear map

$$\phi : \bigotimes_{i=1}^n M_i \longrightarrow M$$

such that $\Phi = \phi \circ \tau_{M_1, \dots, M_n}$.

Definition 11.13 Let M, N be R -modules, $\Phi : M^n = \prod_{i=1}^n M \longrightarrow N$ a multilinear map.

(i) Φ is called *symmetric*, if for any $\sigma \in S_n$ we have

$$\Phi(x_1, \dots, x_n) = \Phi(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

(ii) Φ is called *alternating*, if

$$x_i = x_j \text{ for some } i \neq j \implies \Phi(x_1, \dots, x_n) = 0.$$

If $\text{char}(R) \neq 2$, this is equivalent to

$$\Phi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\Phi(x_1, \dots, x_j, \dots, x_i, \dots, x_n).$$

Proposition 11.14 Let M be an R -module, $n \geq 1$.

(i) There exists an R -module $S^n(M)$, called the n -th symmetric power of M and a symmetric multilinear map

$$\sigma_M^n : M^n \longrightarrow S^n(M)$$

such that for all symmetric, multilinear maps $\Phi : M^n \longrightarrow N$ for any R -module N there exists a unique linear map $\phi : S^n(M) \longrightarrow N$ satisfying $\Phi = \phi \circ \sigma_M^n$.

(ii) There exists an R -module $\Lambda^n(M)$, called the n -th exterior power of M and an alternating multilinear map

$$\lambda_M^n : M^n \longrightarrow \Lambda^n(M)$$

such that for all alternating, multilinear maps $\Phi : \Lambda^n(M) \longrightarrow N$ for any R -module N there exists a unique linear map $\phi : \Lambda^n(M) \longrightarrow N$ satisfying $\Phi = \phi \circ \lambda_M^n$.

proof. (i) Let $T^n(M) = M \otimes_R \dots \otimes_R M$.

Let now $J_n(M)$ be the submodule of $T^n(M)$ generated by all elements

$$(x_1 \otimes \dots \otimes x_n) - (x_{\sigma(1)} \otimes \dots \otimes x_{\sigma(n)}), \quad x_i \in M, \sigma \in S_n$$

Define

$$S^n(M) := T^n(M) / J_n(M), \quad \sigma_M^n := \text{proj} \circ \tau_{M, \dots, M}$$

Then σ_M^n is multilinear and symmetric by construction. Given a multilinear and symmetric map $\Phi : M^n \rightarrow N$, define ϕ as follows: Let $\tilde{\phi} : T^n(M) \rightarrow N$ be the linear map induced by Φ and observe that $J_n(M) \subseteq \ker(\tilde{\phi})$. Hence $\tilde{\phi}$ factors to a linear map

$$\phi : S^n(M) = T^n(M) / J_n(M) \rightarrow N$$

satisfying $\phi \circ \sigma_M^n = \Phi$.

(ii) Similarly let $I_n(M)$ be the submodule of $T^n(M)$ generated by all the elements

$$x_1 \otimes \dots \otimes x_n, \quad x_i \in M \text{ with } x_i = x_j \text{ for some } i \neq j$$

Analogously we define

$$\Lambda^n(M) := T^n(M) / I_n(M), \quad \lambda_M^n := \text{proj} \circ \tau_{M, \dots, M}$$

and obtain the required properties. □

Proposition 11.15 *Let M be a free R -module of rank r and $\{e_1, \dots, e_r\}$ a basis of M . Then $\Lambda^n(M)$ is a free R -module with basis*

$$\text{proj}(e_{i_1} \otimes \dots \otimes e_{i_n}) =: e_{i_1} \wedge \dots \wedge e_{i_n}, \quad 1 \leq i_1 < \dots < i_n \leq r$$

In particular, $\Lambda^n(M) = 0$ for $n > r$ and $\text{rank}(\Lambda^r(M)) = 1$.

proof. By definition we have $e_{i_1} \wedge \dots \wedge e_{i_n} = 0$ if $i_k = i_j$ for some $k \neq j$, hence we have $\Lambda^n(M) = 0$ for $n > r$, as at least one of the e_k must appear twice.

generating: Clearly the $e_{i_1} \wedge \dots \wedge e_{i_n}, i_k \in \{1, \dots, r\}$ generate $\Lambda^n(M)$. We have to show that we can leave out some of them. Obviously $e_{i_{\sigma(1)}} \wedge \dots \wedge e_{i_{\sigma(n)}}$ is a multiple by ± 1 of $e_{i_1} \wedge \dots \wedge e_{i_n}$.

Thus the $e_{i_1} \wedge \dots \wedge e_{i_n}$ with $1 \leq i_1 < i_2 < \dots < i_n \leq r$ generate $\Lambda^n(M)$.

linear independence: Assume

$$\sum_{1 \leq i_1 < \dots < i_n \leq r} a_{i_1, \dots, i_n} e_{i_1} \wedge \dots \wedge e_{i_n} = 0. \quad (*)$$

For fixed $j := (j_1, \dots, j_n), 1 \leq j_1 < \dots < j_n \leq r$ choose $\sigma_j \in S_r$, such that $\sigma_j(k) = j_k$ for

$1 \leq k \leq n$. Then we obtain

$$e_{i_1} \wedge \dots \wedge e_{i_n} \wedge e_{\sigma_j(n+1)} \wedge \dots \wedge e_{\sigma_j(r)} = \begin{cases} \pm e_1 \wedge \dots \wedge e_r, & \text{if } i_k = j_k \text{ for all } k \\ 0 & \text{otherwise} \end{cases}$$

By (*) we get

$$0 = \left(\sum_{1 \leq i_1 < \dots < i_n \leq r} a_{i_1, \dots, i_n} e_{i_1} \wedge \dots \wedge e_{i_n} \right) \wedge e_{\sigma_j(n+1)} \wedge \dots \wedge e_{\sigma_j(r)} = a_j e_{j_1} \wedge \dots \wedge e_{j_r}$$

and thus $a_j = 0$. □

Example 11.16 Let $M = R^n$. Then $\Lambda^k(M)$ is the free R -module with basis

$$e_{i_1} \wedge \dots \wedge e_{i_k}, \quad 1 \leq i_1 < \dots < i_k \leq n$$

and we have $e_1 \wedge e_2 = -e_2 \wedge e_1$. What is $\Lambda^n(R^n) = \Lambda^n(M)$? And what is λ_k^M ? First we obtain $\Lambda^n(R^n) = (e_1 \wedge \dots \wedge e_n)R \cong R$. Then

$$M^n = (R^n)^n = R^{n \times n}, \quad (a_1, \dots, a_n) = A \in R^{n \times n}, \quad a_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} = \sum_{j=1}^n a_{ji} e_j \in R^n = M.$$

For λ_n^M we get

$$\begin{aligned} \lambda_n^M &= \lambda_n^{R^n} = \lambda_n(A) = \lambda_n \left(\sum_{j=1}^n a_{j1} e_j, \dots, \sum_{j=1}^n a_{jn} e_j \right) \\ &= \sum_{j=1}^n a_{j1} e_j \wedge \dots \wedge \sum_{j=1}^n a_{jn} e_j \\ &= \sum_{j=1}^n a_{j1} \left(e_1 \wedge \sum_{j=1}^n a_{j2} e_j \wedge \dots \wedge \sum_{j=1}^n a_{jn} e_j \right) \\ &= \sum_{j=1}^n a_{j1} \cdots \sum_{j=1}^n a_{jn} (e_1 \wedge \dots \wedge e_n) \\ &= \sum_{\sigma \in S_n} a_{\sigma(1)1} \cdots a_{\sigma(n)n} \cdot e_1 \wedge \dots \wedge e_n \cdot \text{sgn}(\sigma) \\ &= \det(A) \cdot e_1 \wedge \dots \wedge e_n, \end{aligned}$$

which is well-known to us.

Definition 11.17 Let M be a R -module. Then we define

$$T(M) := \bigoplus_{n=0}^{\infty} T^n(M), \quad T^0(M) := R, \quad T(M) := M$$

$$S(M) := \bigoplus_{n=0}^{\infty} S^n(M). \quad S^0(M) := R, \quad S(M) := M$$

$$\Lambda(M) := \bigoplus_{n=0}^{\infty} \Lambda^n(M), \quad \Lambda^0(M) := R, \quad \Lambda(M) := M$$

On $T(M)$ define a multiplication

$$\begin{aligned} \cdot : T^n(M) \times T^m(M) &\longrightarrow T^{n+m}(M), \\ (x_1 \otimes \dots \otimes x_n) \cdot (y_1 \otimes \dots \otimes y_m) &\mapsto x_1 \otimes \dots \otimes x_n \otimes y_1 \otimes \dots \otimes y_m \end{aligned}$$

Similarly do it for $S(M)$ and $\Lambda(M)$. Then we have R -algebra-structures and feel free to define

- (i) the *tensor algebra* $T(M)$,
- (ii) the *symmetric algebra* $S(M)$
- (iii) the *exterior algebra* $\Lambda(M)$.

Definition 11.18 Let R be an arbitrary ring.

- (i) An R -algebra is a ring R' together with a ring homomorphism $\alpha : R \longrightarrow R'$. In particular R' is an R -module. If α is injective, R'/R is called a *ring extension*.
- (ii) A homomorphism of R -algebras R', R'' is an R -linear map $\phi : R' \longrightarrow R''$, which is a ring homomorphism.

Example 11.19 (i) $R[X_1, \dots, X_N]$ is an R -algebra for every $n \in \mathbb{N}$.

- (ii) If R' is an R -algebra and $I \trianglelefteq R'$ an ideal, then R'/I is an R -algebra.

Remark 11.20 Let R' be an R -algebra, F a free R -module. Then $F' := F \otimes_R R'$ is a free R' -module.

proof. Let $\{e_i\}_{i \in I}$ be basis of F . Let us show, that $\{e_i \otimes 1\}_{i \in I}$ is basis of F' as an R' -module, where F' is an R' module by

$$b \cdot (x \otimes a) := x \otimes b \cdot a, \quad a, b \in R, \quad x \in F$$

Check the universal property of the free R' -module with basis $\{e_i \otimes 1\}_{i \in I}$ for $F \otimes_R R'$. Let M' be an R' -module and $f : \{e_i \otimes 1\}_{i \in I} \longrightarrow M'$ be a map. We have to show: There exists an R' -linear map $\phi : F' \longrightarrow M'$ with $\phi(e_i \otimes 1) = f(e_i \otimes 1)$. Note that the $\{e_i \otimes 1\}$ generate F' as an R' -module, since $e_i \otimes a = a \cdot (e_i \otimes 1)$ for $a \in R'$. Let $\tilde{\phi} : F \longrightarrow M'$ be the unique R -linear map satisfying $\tilde{\phi}(e_i) = f(e_i \otimes 1)$. Then define

$$\phi : F \otimes_R R' \longrightarrow M', \quad x \otimes a \mapsto a \cdot \tilde{\phi}(x).$$

Then ϕ is R' -linear and we have

$$\phi(e_i \otimes 1) = 1 \cdot \tilde{\phi}(e_i) = \tilde{\phi}(e_i) = f(e_i \otimes 1),$$

which gives us the desired structure of an R' -module. \square

Proposition 11.21 *Let R be a ring, R', R'' two R -algebras.*

(i) $R' \otimes_R R''$ is an R -algebra with multiplication

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) := (a_1 a_2) \otimes (b_1 b_2)$$

(ii) There are R -algebra homomorphisms

$$\sigma' : R' \longrightarrow R' \otimes_R R'', \quad a \mapsto a \otimes 1$$

$$\sigma'' : R'' \longrightarrow R' \otimes_R R'', \quad b \mapsto 1 \otimes b$$

(iii) For any R -algebra A and R -algebra homomorphisms $\phi' : R' \longrightarrow A, \phi'' : R'' \longrightarrow A$, there is a unique R -algebra homomorphism

$$\phi : R' \otimes_R R'' \longrightarrow A$$

satisfying $\phi' = \phi \circ \sigma'$ and $\phi'' = \phi \circ \sigma''$, i.e. making the following diagram commutative

$$\begin{array}{ccc} & & R' \otimes_R R'' \\ & \nearrow \sigma' & \uparrow \sigma'' \\ R' & & R'' \\ & \searrow \phi' & \searrow \phi'' \\ & & A \end{array} \quad \begin{array}{c} | \\ | \\ | \\ | \\ | \\ | \\ \downarrow \phi \end{array}$$

proof. Defining

$$\tilde{\phi} : R' \times R'' \longrightarrow A, \quad (x, y) \mapsto \phi'(x) \cdot \phi''(y)$$

gives us ϕ , which satisfies the required properties. \square

§ 12 Hilbert's basis theorem

Definition 12.1 Let R be a ring, M and R -module.

(i) M is called *noetherian*, if any ascending chain of submodules $M_0 \subset M_1 \subset \dots$ becomes stationary.

- (ii) R is called *noetherian*, if R is noetherian as an R -module, i.e. if every ascending chain of ideals becomes stationary.

Example 12.2 (i) Let k be a field. A k -vector space is noetherian if and only if $\dim(V) < \infty$.
(ii) \mathbb{Z} is noetherian.
(iii) Principle ideal domains are noetherian.

Proposition 12.3 *Let*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

be a short exact sequence. Then M is noetherian if and only if M' and M'' are noetherian.

proof. '⇒' Let M be noetherian. Let first $M'_0 \subset M'_1 \subset \dots$ be an ascending chain of submodules in M' . Then $\alpha(M'_0) \subset \alpha(M'_1) \subset \dots$ is an ascending chain in M . Since M is noetherian, there exists some $n \in \mathbb{N}$, such that $\alpha(M'_i) = \alpha(M'_n)$ for all $i \geq n$. Since α is injective, we have $M'_i = M'_n$ for $i \geq n$, hence M' is noetherian. Let now $M''_0 \subset M''_1 \subset \dots$ be an ascending chain of submodules in M'' . Then $\beta^{-1}(M''_0) \subset \beta^{-1}(M''_1) \subset \dots$ is an ascending chain in M , hence becomes stationary. Since β is surjective, $\beta(\beta^{-1}(M''_i)) = M''_i$ and thus $M''_0 \subset M''_1 \subset \dots$ becomes stationary.

'⇐' Let $M_0 \subset M_1 \subset \dots$ be an ascending chain in M . Let $M'_i := \alpha^{-1}(M_i) \cong M_i \cap M'$ and $M''_i := \beta(M_i)$. By assumption, there exists $n \in \mathbb{N}$, such that $M'_i = M'_n$ and $M''_i = M''_n$ for all $i \geq n$. Then for $i \geq n$ we have

$$\begin{array}{ccccccc} 0 & \longrightarrow & M'_n & \xrightarrow{\alpha} & M_n & \xrightarrow{\beta} & M''_n \longrightarrow 0 & \text{exact} \\ & & \parallel & & \downarrow \gamma & & \parallel & \\ 0 & \longrightarrow & M'_i & \xrightarrow{\alpha} & M_i & \xrightarrow{\beta} & M''_i \longrightarrow 0 & \text{exact} \end{array}$$

Where γ is injective as an embedding. It remains to show that γ is surjective. Let $z \in M_i$. Since β is surjective, there exists $x \in M_n$, such that $\beta(x) = \beta(z)$. Then $\beta(\gamma(x) - z) = 0 \Rightarrow \gamma(x) - z = \alpha(y)$ for some $y \in M'_i = M'_n$. Let $\tilde{x} := x - \alpha(y)$. Then

$$\gamma(\tilde{x}) = \gamma(x) - \gamma(\alpha(y)) = \gamma(x) - \gamma(x) + z = z$$

hence γ is surjective, thus bijective and we have $M_i = M_n$ for $i \geq n$. □

Corollary 12.4 *Let R be a noetherian ring.*

- (i) *Any free R -module F of finite rank n is noetherian.*
(ii) *Any finitely generated R -module M is noetherian.*

proof. (i) Prove this by induction on n .

$n = 1$ Clear.

$n > 1$ Let e_1, \dots, e_n be a basis of F and let F' be the submodule generated by e_1, \dots, e_{n-1} . Then F' is free of rank $n - 1$, thus noetherian by induction hypothesis. Moreover F/F' is free with generator e_n . Thus we have a short exact sequence

$$0 \longrightarrow F' \longrightarrow F \longrightarrow F/F' \longrightarrow 0$$

with $F', F/F'$ noetherian, hence by 12.2, F is noetherian.

- (ii) If M is generated by x_1, \dots, x_n , there is a surjective, R -linear map $\phi: F \longrightarrow M$, sending the e_i to x_i , where F is the free R -module with basis e_1, \dots, e_n . Again by 12.2, M is noetherian which finishes the proof. \square

Proposition 12.5 *For an R -module M the following statements are equivalent:*

- (i) M is noetherian.
- (ii) Any nonempty family of submodules of M has a maximal element with respect to ' \subseteq '.
- (iii) Every submodule of M is finitely generated.

proof. '(i) \Rightarrow (ii)' Let $\mathcal{M} \neq \emptyset$ be a set of submodules of M . Let $M_0 \in \mathcal{M}$. If M_0 is not maximal, there is $M_1 \in \mathcal{M}$ with $M_0 \subsetneq M_1$. If M_1 is not maximal, there is $M_2 \in \mathcal{M}$ with $M_1 \subsetneq M_2$. Since M is noetherian, we come to a maximal submodule M_n after finitely many steps.

'(ii) \Rightarrow (iii)' Let $N \subseteq M$ be a submodule. Let \mathcal{M} be the set of finitely generated submodules of N . Since $(0) \in \mathcal{M}$, we have $\mathcal{M} \neq \emptyset$ and thus there exists a maximal element $N_0 \in \mathcal{M}$. If $N_0 \neq N$, let $x \in N \setminus N_0$ and $N' := N_0 + (x)$ be the submodule generated by N_0 and x . Then clearly $N' \in \mathcal{M}$, which is a contradiction to the maximality of N_0 . Hence $N_0 = N$ and N is finitely generated.

'(iii) \Rightarrow (i)' Let $M_0 \subseteq M_1 \subseteq \dots$ be an ascending chain of submodules in M . Let $N := \bigcup_{n \in \mathbb{N}_0} M_n$. By assumption, N is finitely generated, say by x_1, \dots, x_n . Then there exists $i_0 \in \mathbb{N}$, such that $x_k \in M_{i_0}$ for all $1 \leq k \leq n$. Thus we have $M_i = M_{i_0}$ for $i \geq i_0$, i.e. the chain becomes stationary and M is noetherian. \square

Corollary 12.6 *R is noetherian if and only if every ideal $I \trianglelefteq R$ can be generated by finitely many elements. In particular, every principal ideal domain is noetherian.*

proof. Follows from Proposition 12.4. \square

Theorem 12.7 (Hilbert's basis theorem) *If R is noetherian, $R[X]$ is also noetherian.*

proof. Let $J \trianglelefteq R[X]$ be an ideal. Assume that J is not finitely generated. Let f_1 be an element of $J \setminus \{0\}$ of minimal degree. Then $(f_1) \neq J$. Inductively let $J_i := (f_1, \dots, f_i)$ and pick $f_{i+1} \in J \setminus J_i$ of minimal degree. Let a_i be the leading coefficient of f_i , i.e. we have

$$f_i = a_i X^{\deg(f_i)} + \sum_{j=1}^{\deg(f_i)-1} b_j X^j$$

The ideal $I \trianglelefteq R$ generated by the a_i for $i \in \mathbb{N}$, is finitely generated by assumption. Then we find $n \in \mathbb{N}$ such that $a_{n+1} \in (a_1, \dots, a_n)$, i.e. we have

$$a_{n+1} = \sum_{i=1}^n \lambda_i a_i$$

for suitable $\lambda_i \in R$. Let $d_i := \deg(f_i)$. Note, that $d_{i+1} \geq d_i$ for all $1 \leq i \leq n$. Let now

$$\rho := \sum_{i=1}^n \lambda_i f_i X^{d_{n+1}-d_i}.$$

Then the leading coefficient of ρ is

$$a_{d_{n+1}} = \sum_{i=1}^n \lambda_i a_i$$

Hence $\deg(\rho - f_{n+1}) < d_{n+1}$, $\rho - f_{n+1} \notin J_n$, since $\rho \in J_n$, so f_{n+1} would be in J_n . This contradicts the choice of f_{n+1} . Hence our assumption was false and J is finitely generated and by Corollary 12.5 $R[X]$ is noetherian.

Corollary 12.8 *Let R be noetherian. Then*

- (i) $R[X_1, \dots, X_n]$ is noetherian for any $n \in \mathbb{N}$.
- (ii) Any finitely generated R -algebra is noetherian.

§ 13 Integral ring extensions

Definition 13.1 Let R be ring, S an R -algebra.

- (i) If $R \subseteq S$, S/R is called a *ring extension*.
- (ii) If $R \subseteq S$, $b \in S$ is called *integral over R* , if there exists a monic polynomial $f \in R[X] \setminus \{0\}$ such that $f(b) = 0$.
- (iii) S/R is called an *integral ring extension*, if every $b \in S$ is integral over R .

Example 13.2 (i) If $R = k$ is a field, then *integral* is equivalent to *algebraic*.

- (ii) $\sqrt{2}$ is integral over \mathbb{Z} , since $f = X^2 - 2$ is monic with $f(\sqrt{2}) = 0$.
- (iii) $\frac{1}{2}$ is not integral over \mathbb{Z} .

Assume $\frac{1}{2}$ is integral over \mathbb{Z} . Then there exists some monic $f \in R[X]$, such that $f(\frac{1}{2}) = 0$, i.e. we have

$$\left(\frac{1}{2}\right)^n + g\left(\frac{1}{2}\right) = 0 \quad (*)$$

for some $g \in \mathbb{Z}[X]$. Then $2^{n-1} \cdot g\left(\frac{1}{2}\right) \in \mathbb{Z}$. Multiplying $(*)$ by 2^{n-1} gives us

$$2^{n-1} \cdot \left(\left(\frac{1}{2}\right)^n + g\left(\frac{1}{2}\right) \right) = 0$$

and hence

$$\frac{1}{2} = -2^{n-1} \cdot g\left(\frac{1}{2}\right) \in \mathbb{Z}.$$

Thus $\frac{1}{2}$ is not integral over \mathbb{Z} . More generally, we easily see that any $q \in \mathbb{Q} \setminus \mathbb{Z}$ is not integral over \mathbb{Z} .

Lemma 13.3 *Let S/R be a ring extension, $b \in S$. If $R[b]$ is contained in a subring $S' \subseteq S$ which is finitely generated as an R -module, then b is integral over R .*

proof. Let s_1, \dots, s_n be generators of S' . Since $b \cdot s_i \in S$ (we have $b \in R[b] \subseteq S$), we find $a_{ik} \in R$, such that

$$b \cdot s_i = \sum_{k=1}^n a_{ik} s_k \iff 0 = \sum_{k=1}^n (a_{ik} - \delta_{ik}) s_k. \quad (*)$$

Claim (a) Let A be the coefficient matrix of $(*)$. Then $\det(A) = 0$

Since the determinant is a monic polynomial in b of degree n with coefficients in R , b is integral over R . It remains to show the claim.

(a) Let $A^\#$ be the adjoint matrix

$$A_{ji}^\# = \det(A_{ij} \cdot (-1)^{i+j})$$

where A_{ij} is obtained from A by deleting the i -th row and j -th column. Recall

$$A^\# A = \det(A) \cdot E_n.$$

By $(*)$ we have

$$A \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = 0,$$

hence we have

$$A^\# \cdot A \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = 0 \implies \det(A) \cdot s_i = 0 \quad \text{for all } 1 \leq i \leq n.$$

Since S' is a subring of S , we have $1 \in S'$, hence there exist $\lambda_1, \dots, \lambda_n \in R$ with

$$1 = \sum_{i=1}^n \lambda_i s_i.$$

Finally

$$\det(A) = \det(A) \cdot 1 = \det(A) \cdot \sum_{i=1}^n \lambda_i s_i = \sum_{i=1}^n \det(A) \cdot \lambda_i \cdot s_i = 0$$

Proposition 13.4 Let S/R be a ring extension. Define

$$\overline{R} := \{b \in S \mid b \text{ is integral over } R\} \supseteq R$$

Then \overline{R} is a subring of S , called the *integral closure* of R in S .

proof. Let $b_1, b_2 \in \overline{R}$. We have to show, that $b_1 \pm b_2 \in \overline{R}$, $b_1 b_2 \in \overline{R}$. Let $R[b_1]$ be the smallest subring of S containing R and b_1 . Then R is finitely generated as an R -module by $1, b_1, b_1^2, \dots, b_1^{n-1}$, where n denotes the degree of the 'minimal polynomial' of f . Thus $R[b_1, b_2] = (R[b_1])[b_2]$ is also finitely generated as an $R[b_1]$ -module. This implies, that $R[b_1, b_2]$ is also finitely generated as an R -module and by Lemma 13.2, $R[b_1, b_2]/R$ is an integral ring extension. In particular, $b_1 \pm b_2$ and $b_1 b_2$ are integral over R . \square

Definition 13.5 Let S/R be a ring extension, \overline{R} the integral closure of R in S .

- (i) R is called *integrally closed* in S , if $\overline{R} = R$.
- (ii) Let R be an integral domain. The integral closure of R in $\text{Quot}(R)$ is called the *normalization* of R . R is called *normal*, if it agrees with its normalization.

Proposition 13.6 Any factorial domain is normal.

proof. Let R be a domain and $x = \frac{a}{b} \in \text{Quot}(R)$, $a, b \in R, b \neq 0$ relatively prime. Suppose, x is integral over R , i.e. there exist $\alpha_0, \dots, \alpha_{n-1} \in R$, such that

$$x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_1x + \alpha_0 = 0$$

Multiplying by b^n gives us

$$a^n + \alpha_{n-1}a^{n-1}b + \dots + \alpha_1ab^{n-1} + \alpha_0b^n = 0$$

and hence

$$a^n = b \cdot \underbrace{(-\alpha_{n-1}a^{n-1} - \dots - \alpha_1ab^{n-2} - \alpha_0b^{n-1})}_{\in R} \iff b \mid a^n$$

Since a and b are coprime, we have $b \in R^\times$. Thus $x = \frac{a}{b} = ab^{-1} \in R$ and R is normal. \square

Definition 13.7 Let R be a ring.

- (i) For a prime ideal $\mathfrak{p} \trianglelefteq R$ we define

$$ht(\mathfrak{p}) := \sup\{n \in \mathbb{N}_0 \mid \text{there exist prime ideals } \mathfrak{p}_0, \mathfrak{p}_1, \dots, \mathfrak{p}_n, \text{ with } \mathfrak{p}_n = \mathfrak{p} \text{ and } \mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_n\}$$

to be the *height* of \mathfrak{p} .

- (ii) The *Krull-dimension* of R is

$$\dim(R) := \dim_{\text{Krull}}(R) = \sup\{ht(\mathfrak{p}) \mid \mathfrak{p} \trianglelefteq R \text{ prime}\}$$

Example 13.8 (i) Since $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \dots \subsetneq (X_1, \dots, X_n)$, we have $\dim(k[X_1, \dots, X_n]) \geq n$.

(ii) $\dim(k) = 0$ for any field k , since (0) is the only prime ideal.

(iii) $\dim(\mathbb{Z}) = 1$, since $(0) \subsetneq (p)$ is a maximal chain of prime ideals for $p \in \mathbb{P}$.

(iv) $\dim(R) = 1$ for any principle ideal domain which is not a field:

Assume p, q are prime element with $(p) \subseteq (q)$. Then $p = q \cdot a$ for some $a \in R$. Since p is irreducible, we have $a \in R^\times$ and hence $(p) = (q)$.

(v) $\dim(k[X]) = 1$ for any field k :

Theorem 13.9 (Going up theorem) Let S/R be an integral ring extension and

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$$

a chain of prime ideals in R . Then there exists a chain of prime ideals

$$\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \dots \subsetneq \mathfrak{P}_n$$

in S , such that $\mathfrak{p}_i = \mathfrak{P}_i \cap R$.

proof. Do this by induction on n .

n=0 Let $\mathfrak{p} \triangleleft R$ be a prime ideal. We have to find a prime ideal $\mathfrak{P} \triangleleft S$ with $\mathfrak{P} \cap R = \mathfrak{p}$. Let

$$\mathcal{P} := \{I \triangleleft S \text{ ideal} \mid I \cap R = \mathfrak{p}\}$$

Claim (a) $\mathfrak{p}S \in \mathcal{P}$.

Then \mathcal{P} is nonempty. Zorn's lemma provides us then a maximal element $\mathfrak{m} \in \mathcal{P}$.

Claim (b) $\mathfrak{m} \triangleleft S$ is a prime ideal.

This proves the claim. It remains to show the Claims.

(b) Suppose $b_1, b_2 \in S$ with $b_1 b_2 \in \mathfrak{m}$. Assume $b_1, b_2 \in S \setminus \mathfrak{m}$.

Then $\mathfrak{m} + (b_i) \notin \mathcal{P}$, hence $(\mathfrak{m} + (b_i)) \supsetneq \mathfrak{p}$ for $i \in \{1, 2\}$. \implies Thus there exists $p_i \in \mathfrak{m}, s_i \in S$ such that $r_i := p_i + b_i s_i \in R \setminus \mathfrak{p}$. Then we have

$$r_1 r_2 = (p_1 + b_1 s_1)(p_2 + b_2 s_2) = \underbrace{p_1 p_2 + p_1 b_2 s_2 + b_1 s_1 p_2}_{\in \mathfrak{m}} + \underbrace{b_1 b_2}_{\in \mathfrak{m} \text{ by ass.}} s_1 s_2 \in \mathfrak{m}$$

Clearly $r_1 r_2 \in R$, hence $r_1 r_2 \in \mathfrak{m} \cap R = \mathfrak{p}$, which is a contradiction, since \mathfrak{p} is prime.

(a) We have to show $\mathfrak{p}S \cap R = \mathfrak{p}$. We prove both inclusions.

' \supseteq ' This is clear by definition.

' \subseteq ' Let now

$$b = \sum_{i=0}^n p_i t_i, \quad p_i \in \mathfrak{p}, \quad t_i \in S$$

Since the t_i are integral over R , $R[t_1, \dots, t_n] =: S'$ is finitely generated. Let

s_1, \dots, s_m be generators of S' as an R -module. Since $b \in \mathfrak{p}S'$, we have

$$bs_i = \sum_{k=0}^m a_{ki}s_k$$

for suitable $a_{ik} \in \mathfrak{p}$. Then as in lemma 13.3 we have $\det(a_{ik} - \delta_{ik}b) = 0$ and thus b is a zero of monic polynomial with coefficients in \mathfrak{p} , i.e. b satisfies an equation

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0 \quad \text{with } a_i \in \mathfrak{p},$$

Write

$$b^n = - \sum_{i=0}^{n-1} a_i b^i \in \mathfrak{p},$$

since $b^i \in \mathfrak{p}$. Since \mathfrak{p} is prime, we must have $b \in \mathfrak{p}$ and hence the required inclusion.

n>1 By induction hypothesis we have a chain

$$\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \dots \subsetneq \mathfrak{P}_{n-1}$$

satisfying $\mathfrak{P}_i \cap R = \mathfrak{p}_i$. Moreover we find $\mathfrak{P}_n \triangleleft S$ such that $\mathfrak{P}_n \cap R = \mathfrak{p}_n$. It remains to show $\mathfrak{P}_{n-1} \subsetneq \mathfrak{P}_n$. For $x \in \mathfrak{P}_{n-1}$ we have $x \in R \cap \mathfrak{p}_{n-1}$, i.e. $x \in \mathfrak{p}_{n-1} \subset \mathfrak{p}_n$. Thus $x \in \mathfrak{p}_n \cap R = \mathfrak{P}_n$. Assume now $\mathfrak{P}_{n-1} = \mathfrak{P}_n$. Let $x \in \mathfrak{p}_n$. Then

$$x \in \mathfrak{p}_n \in \mathfrak{p}_n \cap R = \mathfrak{P}_n = \mathfrak{P}_{n-1} = \mathfrak{p}_{n-1} \cap R, \implies x \in \mathfrak{p}_{n-1}$$

and thus $\mathfrak{p}_n \subseteq \mathfrak{p}_{n-1}$, hence $\mathfrak{p}_n = \mathfrak{p}_{n-1}$, a contradiction. \square

Theorem 13.10 *Let S/R be an integral ring extension. Then $\dim(R) = \dim(S)$.*

proof. '≤' Follows from Proposition 13.7

'≥' Let $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \dots \subsetneq \mathfrak{P}_n$ be chain of prime ideals in S and define $\mathfrak{p}_i := \mathfrak{P}_i \cap R$.

Then \mathfrak{p}_i is prime and we have $\mathfrak{p}_i \subseteq \mathfrak{p}_{i+1}$. It remains to show, that $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$.

Define $S' := S/\mathfrak{P}_i$ and $R' := R/\mathfrak{p}_i$. Then S'/R' is integral (!).

We have to show that $\overline{\mathfrak{P}}_{i+1} \cap R = \overline{\mathfrak{p}}_{i+1} :=$ image of \mathfrak{p}_{i+1} in S' is not (0).

Let $b \in \mathfrak{P}_{i+1} \setminus \{0\}$. Since b is integral over R' , there exist $a_0, \dots, a_{n-1} \in R$, such that

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

Let further n be minimal with this property. Write

$$a_0 = -b \cdot \underbrace{(a_1 + a_2b + \dots + a_{n-1}b^{n-2} + b^{n-1})}_{=:c} \in \overline{\mathfrak{P}}_{i+1} \cap R = \overline{\mathfrak{p}}_{i+1}$$

But $c \neq 0$ by the choice of n and $b \neq 0$. Since $R' = R/\mathfrak{p}$ is an integral domain, we have $\bar{0} \neq a_0 \in \bar{\mathfrak{p}}_{i+1}$ and thus $\bar{\mathfrak{p}}_{i+1} \neq (0)$, which proves the claim. \square

Theorem 13.11 (Noether normalization) *Let k be a field. Then every finitely generated k -algebra is an integral extension of a polynomial ring over $k[X]$.*

proof. Let a_1, \dots, a_n be generators of A as a k -algebra. Prove the theorem by induction.

n=1 If a_1 is transcendental over k , then $A \cong k[X]$. Otherwise $A \cong k[X]/(f)$, where f denotes the minimal polynomial of a_1 over k . Thus A is integral over k .

n>1 If a_1, \dots, a_n are algebraically independent, $A \cong k[X_1, \dots, X_n]$. Otherwise there exists some polynomial

$F \in k[X_1, \dots, X_n] \setminus \{0\}$ such that $F(a_1, \dots, a_n) = 0$.

case 1 Assume we have

$$F = X_n^m + \sum_{i=1}^{m-1} g_i X_n^i$$

with $g_i \in k[X_1, \dots, X_n]$. Then $F(a_1, \dots, a_n) = 0$, hence a_n is integral over $A' := k[a_1, \dots, a_{n-1}]$. By induction hypothesis, A' is integral over some polynomial ring, so is A .

case 2 For the general case write

$$F = \sum_{i=0}^m F_i,$$

where F_i is homogenous of degree i , i.e. the sum of the exponents of any monomial in F_i is equal to i . Then replace a_i by $b_i := a_i - \lambda a_n$ (*) with suitable $\lambda_i \in k$, $1 \leq i \leq n-1$. Then $A \cong k[b_1, \dots, b_{n-1}, a_n]$. For any monomial $a_1^{d_1} \cdots a_n^{d_n}$ we find

$$a_1^{d_1} \cdots a_n^{d_n} = (b_1 + \lambda_1 a_n)^{d_1} \cdots (b_{n-1} + \lambda_{n-1} a_n)^{d_{n-1}} \cdot a_n^{d_n} = \left(\prod_{i=1}^{n-1} \lambda_i^{d_i} \right) \cdot a_n^{\sum_{i=1}^n d_i} + \mathcal{O}(a_n)$$

where $\mathcal{O}(a_n)$ denotes terms of lower degree in a_n . Then for $d := \sum_{i=1}^n d_i$ we obtain

$$F_d(a_1, \dots, a_n) = a_n^d \cdot F_d(\lambda_1, \dots, \lambda_{n-1}, 1) + \mathcal{O}(a_n)$$

and thus

$$F(a_1, \dots, a_n) = a_n^m F_m(\lambda_1, \dots, \lambda_{n-1}, 1) + \mathcal{O}(a_n)$$

Choose now $\lambda_1, \dots, \lambda_{n-1} \in k$, such that $F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$. If k is infinite, this is always possible. In the finite case, go back to (*) and use $b_i := a_i + a_n^{\mu_i}$ instead and repeat the procedure. Then by the first case and induction hypothesis the claim follows. \square

§ 14 Dedekind domains

Definition 14.1 A noetherian integral domain R of dimension 1 is called a *Dedekind domain*, if every nonzero ideal $I \triangleleft R$ has a unique representation as a product of prime ideals

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

Definition + remark 14.2 Let R be a noetherian integral domain, $k := \text{Quot}(R)$ and $(0) \neq I \subseteq k$ an R -module.

- (i) I is called a *fractional ideal*, if there exists $a \in R \setminus \{0\}$, such that $a \cdot I \subseteq R$.
- (ii) I is a fractional ideal if and only if I is finitely generated as an R -module.
- (iii) For a fractional ideal I let

$$I^{-1} := \{x \in k \mid x \cdot I \subseteq R\}$$

Then I^{-1} is a fractional ideal.

- (iv) I is called *invertible*, if $I \cdot I^{-1} = R$, where $I \cdot I^{-1}$ denotes the R -module generated by all products $x \cdot y$ with $x \in I, y \in I^{-1}$.

proof. (ii) ' \Rightarrow ' If $a \cdot I \subseteq R$, then $a \cdot I$ is an ideal in R . since R is noetherian, $a \cdot I$ is finitely generated, say by x_1, \dots, x_n . Then I is generated by $\frac{x_1}{a}, \dots, \frac{x_n}{a}$.

' \Leftarrow ' Let y_1, \dots, y_m be generators of I . Write $y_i = \frac{r_i}{a_i}$ with $r_i, a_i \in R \setminus \{0\}$. Define

$$a := \prod_{i=1}^n a_i$$

Then for any generator we have $a \cdot y_i = r \cdot a_1 \cdots a_{i-1} \cdot a_{i+1} \cdots a_m \in R$, hence $a \cdot I \subseteq R$.

Example 14.3 Every principle ideal $I \neq (0)$ is invertible:

Let $I = (a) \trianglelefteq R$. Then $I^{-1} = \frac{1}{a}R$, since we have

$$I \cdot I^{-1} = (a) \cdot \frac{1}{a}R = aR \cdot \frac{1}{a}R = R$$

Proposition 14.4 Let R be a Dedekind domain. Then every nonzero ideal $I \trianglelefteq R$ is invertible.

proof. Let $(0) \neq I \triangleleft R$ be a proper ideal. Then by assumption we can write

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

with prime ideal $\mathfrak{p}_i \triangleleft R$.

If each \mathfrak{p}_i is invertible, then we have

$$I \cdot \mathfrak{p}_r^{-1} \cdots \mathfrak{p}_1^{-1} = R,$$

hence I is invertible. Thus we may assume that $I = \mathfrak{p}$ is prime. Let $a \in \mathfrak{p} \setminus \{0\}$ and write

$$(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_m$$

with prime ideals $\mathfrak{p}_i \triangleleft R$. Then $(a) \subseteq \mathfrak{p}$, i.e. $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some $1 \leq i \leq m$, say $i = 1$. Since the ideals were proper and $\dim(R) = 1$, we have $\mathfrak{p}_1 = \mathfrak{p}$ and $\mathfrak{p}^{-1} = \mathfrak{p}_1^{-1} = \frac{1}{a} \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_m$, since $\mathfrak{p}_1 \mathfrak{p}_1^{-1} = \frac{1}{a}(a) = (1) = R$. \square

Corollary 14.5 *The fractional ideals in a Dedekind domain R form a group.*

proof. Let $(0) \neq I \subseteq k = \text{Quot}(R)$ be a fractional ideal. Choose $a \in R$ such that $a \cdot I \subseteq R$. By Proposition 14.3, $a \cdot I$ is invertible, i.e. there exists a fractional ideal I' , such that

$$(a \cdot I) \cdot I' = R \implies I \cdot (a \cdot I') = R$$

where R is neutral element of the group. \square

Proposition 14.6 *Every Dedekind domain R is normal.*

proof. Let $x \in k := \text{Quot}(R)$ be integral over R , i.e. we can write

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0, \quad a_i \in R$$

By the proof of Proposition 13.3, $R[x]$ is a finitely generated R -module, hence $R[x]$ is a fractional ideal by Remark 14.2. Further by Corollary 14.4 $R[x]$ is invertible, i.e. we can find $I \triangleleft k$, such that $I \cdot R[x] = R$.

On the other hand $R[x]$ is a ring, i.e. $R[x] \cdot R[x] = R[x]$. Multiplying the equation by I gives us $x \in R$. In particular we have

$$R = I \cdot R[x] = I \cdot (R[x] \cdot R[x]) = (I \cdot R[x]) \cdot R[x] = R \cdot R[x] = R[x],$$

which implies the claim. \square

Proposition 14.7 *Let R be noetherian integral domain of dimension 1. Then R is a Dedekind domain if and only if R is normal.*

proof. ' \Rightarrow ' This is Proposition 14.5

' \Leftarrow ' We claim

claim (a) For every prime ideal $(0) \neq \mathfrak{p} \triangleleft R$ the localization $R_{\mathfrak{p}}$ is a discrete valuation ring.

claim (b) Every nonzero ideal in R is invertible.

Then let $(0) \neq I \neq R$ be an ideal in R . Then $I \subseteq \mathfrak{m}_0$ for a maximal ideal $\mathfrak{m}_0 \triangleleft R$. By claim (b), \mathfrak{m}_0 is invertible. Define $I_1 := \mathfrak{m}_0^{-1} \cdot I$. Then $I_1 \subseteq \mathfrak{m}_0^{-1} \cdot \mathfrak{m}_0 = R$ is an ideal. If $I_1 = R$, then

$I = \mathfrak{m}_0$. Otherwise let \mathfrak{m}_1 be a maximal ideal containing I_1 and define $I_2 := \mathfrak{m}_1^{-1} \cdot I_1 \triangleleft R$. If $I_1 = I$, then $\mathfrak{m}_0^{-1} \cdot I = I \xrightarrow{\text{invert.}} \mathfrak{m}_0^{-1} = R$, which is a contradiction.

By this way we obtain a chain of ideals

$$I \subsetneq I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_n$$

Since R is noetherian, there exists $n \in \mathbb{N}$; such that $I_n = R$. Then

$$R = I_n = \mathfrak{m}_{n-1}^{-1} \cdot I_{n-1} = \mathfrak{m}_{n-1}^{-1} \cdot \mathfrak{m}_{n-1}^{-1} \cdot I_{n-2} = \mathfrak{m}_{n-1}^{-1} \cdots \mathfrak{m}_0^{-1} \cdot I$$

Thus

$$I = \mathfrak{m}_0 \cdot \mathfrak{m}_1 \cdots \mathfrak{m}_{n-2} \cdot \mathfrak{m}_{n-1}$$

with maximal, thus prime ideals \mathfrak{m}_i . Hence R is a Dedekind domain.

It remains to show the claims.

(b) Let $(0) \neq I \triangleleft R$ be an ideal. We have to show $I \cdot I^{-1} = R$ for $I^{-1} = \{x \in k \mid x \cdot I \subseteq R\}$.

' \subseteq ' Clear.

' \supseteq ' Assume $I \cdot I^{-1} \neq R$. Then there exists a maximal ideal $\mathfrak{m} \triangleleft R$ such that $I \cdot I^{-1} \subseteq \mathfrak{m}$.

By claim (a), $R_{\mathfrak{m}}$ is a principal ideal domain, thus $I \cdot R_{\mathfrak{m}}$ is generated by one element, say $\frac{a}{s}$ for some $a \in I, s \in R \setminus \mathfrak{m}$. Let now b_1, \dots, b_n be generators of I as an ideal in R .

Then

$$\frac{b_i}{1} = \frac{a}{s} \cdot \frac{r_i}{s_i}, \quad r_i \in R, s_i \in R \setminus \mathfrak{m}, \quad \text{for } 1 \leq i \leq n$$

Define $t := s \cdot s_1 \cdots s_n \in R \setminus \mathfrak{m}$.

We have $\frac{t}{a} \in I^{-1}$, since

$$\frac{t}{a} \cdot b_i = \frac{t}{a} \cdot \frac{a}{s} \cdot \frac{r_i}{s_i} = r_i \cdot s_1 \cdots s_{i-1} \cdot s_{i+1} \cdots s_n \in R$$

for $1 \leq i \leq n$. But then

$$t = \frac{t}{a} \cdot a \in I^{-1} \cdot I \subseteq \mathfrak{m} \quad \nmid$$

(a) We will only give a proof sketch. The strategy is as follows:

(i) It suffices to show, that $\mathfrak{m} := \mathfrak{p}R_{\mathfrak{p}}$ is a principal ideal.

(ii) Show that $\mathfrak{m}^n \neq \mathfrak{m}$.

(iii) Show that \mathfrak{m} is invertible.

Then pick $t \in \mathfrak{m}^2 \setminus \mathfrak{m}$ and obtain $t \cdot \mathfrak{m}^{-1} = R_{\mathfrak{p}}$. This is true, since otherwise, as \mathfrak{m} is the only maximal ideal in $R_{\mathfrak{p}}$, we would have $t \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{m}$ and thus $t \in \mathfrak{m}^2$, which implies $\mathfrak{m} = \mathfrak{m}^2$.

Then we have

$$(t) = t \cdot R = t \cdot (\mathfrak{m} \cdot \mathfrak{m}^{-1}) = R_{\mathfrak{p}} \cdot \mathfrak{m} = \mathfrak{m},$$

which will give us the claim. □

Theorem 14.8 *Let R be a Dedekind domain, L/k a finite separable field extension of $k := \text{Quot}(R)$ and S the integral closure of R in L . Then S is a Dedekind domain.*

proof. We will show all the required properties of a Dedekind domain.

integral domain. This is clear.

dimension 1. We know that S/R is integral and Proposition 13.7 gives us $\dim(S) = 1$.

normal. If $x \in L$ is integral over S , x is integral over R , thus $x \in S$.

noetherian. This is the only hard work in the proof. Let $N := [L : k]$. Since L/k is separable, there exists $\alpha \in L$ such that $L = k(\alpha)$. Moreover we have $|\text{Hom}_k(L, \bar{k})| = n$, say $\text{Hom}_k(L, \bar{k}) = \{\text{id} = \sigma_1, \dots, \sigma_n\}$.

claim (a) α can be chosen in S .

Then let

$$D := \begin{pmatrix} 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \sigma_2(\alpha) & \dots & \sigma_2(\alpha^{n-1}) \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\alpha) & \dots & \sigma_n(\alpha^{n-1}) \end{pmatrix} = (\sigma_i(\alpha^j))_{(i,j) \in \{1, \dots, n\} \times \{0, \dots, n-1\}}$$

and $d := (\det(D))^2$. $d := d_{L/k}(\alpha)$ is called the *discriminant of L/k with respect to α* .

claim (b) We have

(i) $d \neq 0$

(ii) S is contained in the R -module generated by $\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{n-1}}{d}$.

Then S is submodule of a finitely generated R -module, and since R is noetherian, S is noetherian as an R -module, thus also as an S -module. This proves *noetherian*. Now prove the claims.

(a) Let $\tilde{\alpha} \in L$ be a primitive element, i.e. $L = k(\tilde{\alpha})$. Let

$$f = X^n - \sum_{i=0}^{n-1} c_i X^i$$

be the minimal polynomial of $\tilde{\alpha}$ over k . Write $c_i = \frac{a_i}{b_i}$ for suitable $a_i, b_i \in R, b_i \neq 0$. Now define

$$b := \prod_{i=0}^{n-1} b_i, \quad \alpha := b \cdot \tilde{\alpha}.$$

Since we have

$$\alpha^n = b^n \tilde{\alpha}^n = b^n \cdot \sum_{i=0}^{n-1} c_i \tilde{\alpha}^i = \sum_{i=0}^{n-1} c_i \cdot \frac{\alpha^i}{b^i} b^n$$

we obtain

$$\alpha^n = b^n \cdot \tilde{\alpha}^n = \sum_{i=0}^{n-1} c_i' \alpha^i, \quad c_i' = c_i \cdot b^{n-i} \in R.$$

Thus α is integral over R , i.e. $\alpha \in S$. We easily see $k(\alpha) = k(\tilde{\alpha})$, hence the claim is proved.

(b) (i) We have

$$d = (\det(D))^2 = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \neq 0,$$

since otherwise we would have $\sigma_i(\alpha) = \sigma_j(\alpha)$, i.e.e $\sigma_i = \sigma_j$, which is not possible.

(ii) Let $\beta \in S$. Write

$$\beta = \sum_{i=0}^{n-1} c_{i+1} \alpha^i, \quad c_i \in k.$$

We have to show: $c_i \in \frac{1}{d}R$ for all $1 \leq i \leq n$. Therefore we need

claim (c) There is a matrix $A \in R^{n \times n}$ and $b \in R^n$, such that

$$A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = b \quad \text{and} \quad \det(A) = d.$$

Then by Cramer's rule and Claim (c) we have

$$c_i = \frac{\det(A_i)}{\det(A)} = \frac{\det(A_i)}{d} \in \frac{1}{d}R \in R$$

where A_i is obtained by replacing the i -th column of A by b . This proves claim (b).

(c) Recall that

$$tr_{L/k} : L \longrightarrow k, \quad \beta \mapsto \sum_{i=1}^n \sigma_i(\beta)$$

is a k -linear map. For β as above we find for $1 \leq i \leq n$

$$(*) \quad tr_{L/k}(\underbrace{\alpha^{i-1} \beta}_{\in S}) = \sum_{j=1}^n tr_{L/k}(\alpha^{i-1} \alpha^{j-1} c_j) = \sum_{j=1}^n tr_{L/k}(\alpha^{i-1} \alpha^{j-1}) c_j \in k \cap S = R$$

where the last equality holds since R is normal and by Proposition 14.5. Let now

$$A = (a_{ij})_{(i,j) \in \{1, \dots, n\} \times \{1, \dots, n\}}, \quad a_{ij} = tr_{L/k}(\alpha^{i-1}, \alpha^{j-1})$$

and

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \quad b_i = tr_{L/k}(\alpha^{i-1} \beta).$$

Then by (*) we have

$$A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = b,$$

i.e. the first part of the claim. Moreover we have $D^T D = (\tilde{a}_{ij})$, where

$$\tilde{a}_{ij} = \sum_{k=1}^n \sigma_k(\alpha^{i-1}) \sigma_k(\alpha^{j-1}) = \sum_{k=1}^n \sigma_k(\alpha^{i-1} \alpha^{j-1}) = \text{tr}_{L/k}(\alpha^{i-1}, \alpha^{j-1}) = a_{ij}.$$

Hence $D^T D = A$ and by $\det(D) = \det(D^T)$ we have

$$\det(D)^2 = \det(D \cdot D) = \det(D \cdot D^T) = \det(A) = d.$$

We have now shown that S is an integral domain, of dimension 1, noetherian and normal. By Proposition 14.6 the theorem is proved. \square