

Chapter 1

Ideals and Divisibility

Notation:

Semigroup: commutative semigroup with unit element (i.e. non-empty set together with a binary, associative, commutative operation having a unit element).

Monoid: semigroup satisfying the cancellation law (i.e. $\forall a, b, c (ab = ac \Rightarrow b = c)$).

Ring: commutative ring with unit element.

All the semigroup/ring homomorphisms respect the unit element.

Let M be a monoid. We define the following notions:

$M^\times = \{x \in M \mid \exists y \in M (xy = 1)\}$ is the **unit group** of M .

M is called **reduced** if $M^\times = \{1\}$. M is a **group** if $M^\times = M$.

A group Q is called a **quotient group** for M if $M \subseteq Q$ and $Q = \{ab^{-1} \mid a, b \in M\}$.

Every monoid has a quotient group $q(M)$. Every multiplicatively closed subset of an abelian group is a monoid.

Let R be a ring. We define:

$R^\times = \{x \in R \mid \exists y \in R (xy = 1_R)\}$ is the **unit group** of R .

$R^\circ = R \setminus \{0\}$.

$\text{Zdv}(R) = \{x \in R \mid \exists y \in R^\circ (xy = 0_R)\}$ is the set of **zero divisors** of R . We have:

- $R = \{0\} \iff 0 = 1$.
- $0 \in \text{Zdv}(R) \iff R \neq \{0\}$.
- $R^\times \cap \text{Zdv}(R) = \emptyset$ (if $a \in R^\times$, $x \in R$ and $ax = 0$, then $x = 1 \cdot x = a^{-1}ax = a^{-1}0 = 0$).

A subset $T \subseteq R$ is called **multiplicatively closed** if $1 \in T$ and $a, b \in T \Rightarrow ab \in T$.

R is called an **integral domain** (or just **domain**) if $\text{Zdv}(R) = \{0\}$ ($\iff R^\circ$ is multiplicatively closed $\iff R^\circ \subseteq R$ is a semigroup (if this holds, then R° is a monoid)). R is called a **field** if $R^\circ = R^\times$. Every subring of a field is a domain.

A field K is called a **quotient field** of R if $R \subseteq K$ and $K = \{ab^{-1} \mid a, b \in R, b \neq 0\}$. It can be proved that every domain R has a quotient field $\mathbf{q}(R)$ and that every finite domain is a field.

Algebraic number field: field extension K/\mathbb{Q} of finite degree (i.e. there is an $\alpha \in K$ s.t. $K = \mathbb{Q}(\alpha)$, $[K : \mathbb{Q}] := \dim_{\mathbb{Q}} K = \deg(\text{minimal polynomial of } \alpha \text{ over } \mathbb{Q})$).

Examples:

- $a = \sqrt{d}, d \in \mathbb{Z}^\circ$ squarefree. $R = \mathbb{Z}[\sqrt{d}] \subseteq K = \mathbb{Q}(\alpha)$.
- $\alpha = \xi_n = e^{\frac{2\pi i}{n}}$. $R = \mathbb{Z}[\xi_n] \subseteq \mathbb{Q}(\xi_n)$.

1.1 Divisibility

If R is a domain, then R° is a monoid. We are going to define all the concepts of divisibility for monoids, and use them for domains.

Let M be a monoid and $a, b \in M$. We say that a **divides** b , in symbols $a|b$, if $\exists c \in M (ac = b)$.

Two elements are called *associated* if $a|b$ and $b|a$ (equivalently, if $aM^\times := \{a\varepsilon \mid \varepsilon \in M^\times\} = bM^\times$; equivalently, if $b \in aM^\times$). Of course “to be associated” is an equivalence relation on M , and the equivalence class of an element a is precisely aM^\times .

An element $p \in M$ is called

- **irreducible** (or **atom**) in M if $p \notin M^\times$ and $\forall a, b \in M (p = ab \Rightarrow a \in M^\times \vee b \in M^\times)$.
- **prime** in M if $p \notin M^\times$ and $\forall a, b \in M (p|ab \Rightarrow p|a \vee p|b)$.

$\mathcal{A}(M)$ is the **set of atoms**.

It can be proved that every prime element is irreducible.

Examples. (we use the following notation: $\mathbb{N} = \{1, 2, \dots\}$ and $\mathbb{N}_0 = \{0, 1, 2, \dots\}$.)

- $M = (\mathbb{N}, \cdot)$
- $M = (4\mathbb{N}_0 + 1, \cdot)$. Observe that $9 \in M$ is irreducible, but not prime, since $9|9 \cdot 49 = 21 \cdot 21$.

A monoid is called

- **atomic** if every $a \in M \setminus M^\times$ has a factorization into atoms (i.e. $\forall a \in M \setminus M^\times \exists l \in \mathbb{N} \exists u_1, \dots, u_l \in \mathcal{A}(M)$ s.t. $a = u_1 \cdot \dots \cdot u_l$). Observe that such a factorization might not be unique.
- *factorial*, if every $a \in M \setminus M^\times$ has a factorization into primes.

Of course, every factorial monoid is atomic.

Addendum. Observe that, a priori, in a factorial monoid the factorization might not be unique. Nevertheless, the following holds (cfr. [1], p. 209):

Proposition. Let M be a monoid. The following conditions are equivalent:

1. M is factorial.
2. M is atomic and every atom is prime.
3. Every $a \in M \setminus M^\times$ is a product of atoms, and this factorization is unique up to associates and order (cfr. Lemma 1.3).

A domain is called *atomic* (resp. *factorial*) if the monoid (R°, \cdot) is atomic (resp. factorial).

Examples.

1. Fundamental Theorem of Arithmetic: (\mathbb{N}, \cdot) is factorial (and \mathbb{Z} is factorial).
2. Every Euclidean domain¹ is factorial. The polynomial ring over a field in one indeterminate is Euclidean with $\delta := \deg$.
3. $M = (4\mathbb{N}_0 + 1, \cdot)$ is not factorial, since $21 \cdot 21 = 9 \cdot 49$. (??? e allora? 21 e 9 mica sono primi...)
4. $R = \mathbb{Z}[\sqrt{-5}]$ is not atomic, since $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$, and all the factors are irreducible and non-associated. (NOTA: aggiungere dimostrazione in appendice)

Definition 1.1. Let M be a monoid and $A \subseteq M$ a subset.

1. An element $d \in M$ is called a *greatest common divisor* of A if the following two conditions are satisfied:
 - (i) $d|a$ for all $a \in A$.

¹Recall the definition of *Euclidean domain*: a ring R is an Euclidean domain if there exists a map $\delta : R^\circ \rightarrow \mathbb{N}_0$ s.t. $\forall a, b \in R^\circ \exists q, r$ s.t. $a = bq + r$ and $r = 0$ or $\delta(r) < \delta(b)$. Such a δ is called *euclidean norm*, and it's not necessarily unique.

(ii) If $e \in M$ and $e|a$ for all $a \in A$, then $e|d$.

We define $\gcd_M(A)$ as the set of all greatest common divisors of A .

2. M is called a *GCD-monoid* if $\gcd_M(A) \neq \emptyset$ for all $\emptyset \neq A \subseteq M$ finite. A domain R is a *GCD-domain* if R° is a GCD-monoid.

Examples. For any monoid, consider the set of prime elements. We are interested in a set \mathbb{P} of representatives² for the equivalence relation of “being associate” on the set of primes.

- $H = (\mathbb{Z}^\circ, \cdot)$. Since $\mathbb{Z}^\times = \{-1, 1\}$, a possible candidate for \mathbb{P} is $\{2, 3, 5, 7, \dots\}$. Of course also $\{2, -3, -5, 7, 11, -13, \dots\}$ works.
- $R = K[X]$ is factorial. It can be proved that $R^\times = K^\times$. We can define \mathbb{P} as the set of irreducible polynomials with leading coefficient 1.

Lemma 1.2. Let M be a GCD-monoid. The following hold:

1. If $A \subseteq M$ and $d \in \gcd(A)$, then $\gcd(A) = dM^\times$.
2. If $a, b, c \in M$ with $a|bc$, then $a = b'c'$ for some $b', c' \in M$ s.t. $b'|b$ and $c'|c$.
3. If $a, b, c \in M$ with $a|bc$ and $\gcd(a, b) = M^\times$, then $a|c$.
4. Every atom is prime.

Proof.

1. To show “ \subseteq ”, observe that if $d' \in \gcd(A)$, then $d|d'$ and $d'|d$, hence $d' \in dM^\times$. As for “ \supseteq ”, let $u \in M^\times$. Observe that
 - (i) If $a \in A$, then $d|a$ and so $du|a$.
 - (ii) If $e \in M$ with $e|a$ for all $a \in A$, then $e|d$ and thus $e|du$.

Therefore $du \in \gcd(A)$.

2. We give no proof for the result, although it’s not completely trivial.
3. By second point, we have $a = b'c'$ with $b'|b$ and $c'|c$. Then b' divides both a and b , whereby $b'|1$, i.e. b' is a unit. Hence $a|c'|c$.
4. Let p be an atom and $b, c \in M$ with $p|bc$. Second point implies that $p = b'c'$ with $b'|b$ and $c'|c$. Since p is an atom, we can assume w.l.o.g. that b' is a unit, whereby $p|c$.

²Observe that, if the Axiom of Choice holds, such a set always exists.

□

Let's denote with " \simeq " the equivalence relation of "being associate".

Lemma 1.3 (Properties of prime elements). Let M be a monoid.

1. Let $m, n \in \mathbb{N}_0$ and let $p_1, \dots, p_n, q_1, \dots, q_m \in M$ be primes. Let $c, d \in M$ be such that $p_i \nmid d$ and $q_j \nmid c$ for all $i \in [1, n], j \in [1, m]$. Suppose $p_1 \cdot \dots \cdot p_n \cdot c \simeq q_1 \cdot \dots \cdot q_m \cdot d$. Then $m = n$, and there is a bijection $\sigma \in S_n$ such that $q_{\sigma(i)} \simeq p_i$ for $i \in [1, n]$.
2. Let M be atomic and $P \subseteq M$ a set of prime elements. Then every $a \in M$ may be written in the form $a = p_1 \cdot \dots \cdot p_n \cdot c$, with $n \in \mathbb{N}$, $p_1, \dots, p_n \in P$ and $c \in M$, where c is not divisible by any $p \in P$. Furthermore, p_1, \dots, p_n and c are uniquely determined (up to the order and up to associates).
3. Let M be atomic, $p \in M$ prime, and $a \in \mathfrak{q}(M)$. Then there exist $b, c \in M$ and $n \in \mathbb{Z}$ s.t. $a = p^n c^{-1} b$ with $p \nmid bc$. Furthermore, the exponent n is uniquely determined by aM^\times and pM^\times .

Proof.

1. We proceed by induction on n . If $n = 0$, then necessarily $m = 0$, and we are done. Suppose now $n > 0$. Then $p_1 \mid q_1 \cdot \dots \cdot q_m d$, and since $p_1 \nmid d$ we obtain by primality that $p_1 \mid q_j$ for some $j \in [1, m]$. Since $p_1, q_j \in \mathcal{A}(M)$, we get $p_1 \simeq q_j$ and hence

$$p_2 \cdot \dots \cdot p_n \cdot c \simeq q_1 \cdot \dots \cdot q_{j-1} \cdot q_{j+1} \cdot \dots \cdot q_m \cdot d.$$

Now the assertion follows immediately by the induction hypothesis.

2. By first point, it is sufficient to show the existence of such a factorization. Let $a \in M$. Then $a = \varepsilon \cdot r_1 \cdot \dots \cdot r_n$, where $n \in \mathbb{N}_0$ and $r_1, \dots, r_n \in \mathcal{A}(M)$. After renumbering if necessary, there is an $m \in [0, n]$ such that w.l.o.g. $r_j \in P$ for each $j \in [1, m]$ and $r_j \not\in P$ for any $p \in P$, $j \in [m+1, n]$. Thus the assertion holds with $c = \varepsilon \cdot r_{m+1} \cdot \dots \cdot r_n$.

3. Existence: If $a \in M$, then (by second point with $P := \{p\}$) there exist $n \in \mathbb{N}_0$ and $b \in M$ s.t. $p \nmid b$ and $a = p^n b$.

If $a \in \mathfrak{q}(M)$, then $a = a_0^{-1} a_1$ for some $a_0, a_1 \in M$. For $i \in \{0, 1\}$, we can write $a_i = p^{n_i} b_i$ and hence $a = p^{n_1 - n_0} b_0^{-1} b_1$, where $p \nmid b_0 b_1$.

Uniqueness: Let a and p be the same of above. Let $a_1 = va$ and $p_1 = up$ with $u, v \in M^\times$. We can write $a = p^n c^{-1} b$ and $a_1 = p_1^{n_1} c_1^{-1} b_1$, where $n, n_1 \in \mathbb{Z}$,

$b, c, b_1, c_1 \in M$, $p \nmid bc$ and $p_1 \nmid b_1 c_1$.

Let $k \in \mathbb{N}_0$ be such that $k + n \geq 0$ and $k + n_1 \geq 0$. Then

$$vp^n \frac{b}{c} = va = a_1 = (up)^{n_1} \frac{b_1}{c_1},$$

whereby $p^{n+k} c_1 vb = p^{n_1+k} cu^{n_1} b_1$, and it's an element of M . Hence (by second point with $P := \{p\}$) we get $n + k = n_1 + k$, i.e. $n = n_1$. □

The third point of Lemma 1.3 assures that the following function is well defined:

Definition 1.4. For any $p \in M$ prime, the map $v_p : \mathbf{q}(M) \rightarrow \mathbb{Z}$ given by $p^n c^{-1} b \mapsto n$ is called the *p-adic valuation* of M . We have $v_p[M] = \mathbb{N}_0$ and v_p is a homomorphism.

Lemma 1.5. Let M be a monoid and P a set of representatives of prime elements of M . The following are equivalent:

- (a) M is factorial.
- (b) Every $a \in M \setminus M^\times$ is a product of primes, and the representation is unique up to associates and up to the order. In particular

$$a = \varepsilon \prod_{p \in P} p^{v_p(a)}$$

for some $\varepsilon \in M^\times$.

- (c) M is atomic and $\gcd(A) \neq \emptyset$ for all $\emptyset \neq A \subseteq M$ finite.
- (d) M is atomic, and every atom is prime.

Furthermore, if M is factorial and $\emptyset \neq A \subseteq M$, then

$$\gcd(A) = \prod_{p \in P} p^{\min\{v_p(a) \mid a \in A\}} M^\times \quad (*)$$

Proof.

(a) \Rightarrow (b): For free by Lemma 1.3.

(b) \Rightarrow (c): It is sufficient to prove (*). By Lemma 1.2 it suffices to show that

$$d := \prod_{p \in P} p^{\min\{v_p(a) \mid a \in A\}} \in \gcd(A).$$

First check (easy exercise) that for any $a, b \in M$ the following holds:

$$a \mid b \text{ if and only if } v_p(a) \leq v_p(b) \text{ for all } p \in P.$$

By this it follows easily (exercise) that d satisfies the definition of \gcd .

(c) \Rightarrow (d): For free by Lemma 1.2(4).

(d) \Rightarrow (a): Trivial by definition. □

1.2 Rings and Ideals

Let R be a ring and $I, J \triangleleft R$ ideals. Then $I \cap J$, $I + J := \{a + b \mid a \in I, b \in J\}$ and $IJ := \{\sum_{i=1}^m a_i b_i \mid m \in \mathbb{N}_0, a_i \in I, b_i \in J\} = {}_R\langle ab \mid a \in I, b \in J \rangle$ are ideals.

We define the following objects:

- $(\mathcal{F}(R), \cdot)$ is the *semigroup of ideals of R* . The unit element is $R = {}_R\langle 1 \rangle$.
- $(\mathcal{F}^\circ(R), \cdot)$ is the *set of non-zero ideals of R* .
- $(\mathcal{H}(R), \cdot)$ is the *set of non-zero principal ideals of R* .

If R is a domain, then $\mathcal{H}(R) \subseteq \mathcal{F}^\circ(R) \subseteq \mathcal{F}(R)$ are (sub)monoids.

The function $\theta : R^\circ/R^\times \rightarrow \mathcal{H}(R)$ given by $a \mapsto aR$ is a semigroup isomorphism.

If $K := \mathfrak{q}(R^\circ)$, the group $K^\times/R^\times = \mathfrak{q}(R^\circ/R^\times) \simeq \mathfrak{q}(\mathcal{H}(R)) = \{aR \mid a \in K^\times\}$ is called *group of divisibility*.

Lemma 1.6. Let $I \subsetneq R$ be an ideal. The following are equivalent:

- R/I is a domain.
- If $a, b \in R$ and $ab \in I$, then $a \in I$ or $b \in I$.
- If $A, B \triangleleft R$ and $AB \subseteq I$, then $A \subseteq I$ or $B \subseteq I$.
- $R \setminus I$ is multiplicatively closed.

Proof.

(a) \Leftrightarrow (b): Well known³

(b) \Leftrightarrow (d): Trivial by definition.

(c) \Rightarrow (b): It's sufficient to consider singletons.

(b) \Rightarrow (c): By contraposition. Suppose $AB \subseteq I$, $A \not\subseteq I$ and $B \not\subseteq I$. Then there are $a \in A \setminus I$, $b \in B \setminus I$ and $ab \in AB \subseteq I$, i.e. \neg (b). \square

Definition 1.7. An ideal $I \subseteq R$ is called

- *prime* if $I \neq R$ and one of the equivalent statements of Lemma 1.6 holds.
- *maximal* If $I \neq R$ and there are no ideals $J \subseteq R$ s.t. $I \subsetneq J \subsetneq R$.

It is a well-know result that an ideal $I \triangleleft R$ is maximal if and only if R/I is a field⁴.

The following results should be already known by the reader.

³See https://proofwiki.org/wiki/Prime_Ideal_iff_Quotient_Ring_is_Integral_Domain.

⁴See https://proofwiki.org/wiki/Maximal_Ideal_iff_Quotient_Ring_is_Field.

Remark 1.8.

1. Every maximal ideal is prime.
2. Let R be a domain and $p \in R^\circ$. Then $pR \triangleleft R$ is prime iff $p \in R$ is a prime element.
3. $\{0\} \subseteq R$ is a prime ideal iff R is a domain.
4. We denote by $\text{Spec}(R)$ the set of prime ideals, and by $\text{max}(R)$ the set of maximal ideals.
5. Let R be a domain. Then R is factorial $\stackrel{\text{def}}{\Leftrightarrow} (R^\circ, \cdot)$ is factorial $\Leftrightarrow (\mathcal{H}(R), \cdot)$ is factorial.

Lemma 1.9. Let R be a PID (principal ideal domain). The following hold:

1. $\{pR \mid p \in R \text{ is prime}\} = \text{Spec}(R) \setminus \{(0)\}$.
2. $\text{Spec}(R) \setminus \{(0)\} = \text{max}(R)$.
3. $\mathcal{F}^\circ(R) = \mathcal{H}(R)$, it is factorial and $\text{Spec}(R) \setminus \{(0)\}$ is the set of prime elements of $\mathcal{F}^\circ(R)$.

Proof.

1. See point (2) of previous remark.
2. It suffices to show “ \subseteq ”. Let $p \in R$ be prime and $I = bR \triangleleft R$ such that $pR \subsetneq bR \triangleleft R$. We have to show that $I = R$. Since $p \in bR$, we get $p = bc$ for some $c \in R$. Since $b \notin pR$, this implies $p|c$, i.e. $c = pd$ for some $d \in R$. Then $p = bpd$, which means that $b \in R^\times$, thus $bR = I = R$.
3. Exercise.

□

Remark.

1. In general, a domain (and even a factorial domain) need not be a principal ideal domain:
 - Let K be a field. Then $K[X, Y]$ is a factorial domain. Since $K[X, Y]/\langle X \rangle \simeq K[Y]$, which is a domain, the ideal $\langle X \rangle$ is prime, but of course is not maximal (since $\langle X \rangle \subsetneq \langle X, Y^2 \rangle \subsetneq K[X, Y]$).
 - $R = \mathbb{Z}[X]$ is factorial, but for $p \in \mathbb{P}$ the ideal ${}_R\langle p, X \rangle$ is not a principal ideal.

2. A domain R is called a *Dedekind domain* if $\mathcal{F}^\circ(R)$ is factorial (and then $\text{Spec}(R) \setminus \{(0)\}$ is the set of prime elements).
The rings of integers in algebraic number fields are Dedekind domains (e.g. $\mathbb{Z}[\xi_n] \subseteq \mathbb{Q}(\xi_n)$).

Chapter 2

An introduction to Module Theory

Throughout this whole chapter, R is a ring.

2.1 Submodules, factor modules and homomorphisms.

2.1.1 Submodules.

Definition 2.1. Let $(M, +)$ be an additive abelian group. An R -module structure on M is a map

$$\begin{aligned} R \times M &\rightarrow M \\ (\lambda, x) &\mapsto \lambda \cdot x = \lambda x \end{aligned}$$

such that for all $\lambda, \mu \in R$ and all $x, y \in M$ the following conditions hold:

1. $1 \cdot x = x$.
2. $(\lambda\mu)x = \lambda(\mu x)$.
3. $\lambda(x + y) = \lambda x + \lambda y$.
4. $(\lambda + \mu)x = \lambda x + \mu x$.

An R -module M is an additive abelian group together with an R -module structure (also called *scalar multiplication*).

Remarks and Examples.

1. If $\lambda \in R$, then $\lambda 0 = \lambda(0 + 0) = \lambda 0 + \lambda 0$, and hence $\lambda 0 = 0$.

2. If R is a field, then an R -module is an R -vector space.
3. Set $R = \mathbb{Z}$. Every abelian group is a \mathbb{Z} -module (with the usual integer multiplication as scalar multiplication).
4. The ring multiplication $R \times R \rightarrow R$, $(x, y) \mapsto x \cdot_R y$ is an R -module structure, i.e. R is an R -module.
5. Let $f : R \rightarrow S$ be a ring homomorphism. Then S is an R -module with the structure

$$\begin{aligned} R \times S &\rightarrow S \\ (r, s) &\mapsto f(r)s. \end{aligned}$$

In particular, if $R \subseteq S$ is a subring, then S is an R -module by ring multiplication (e.g. $R \subseteq R[X_1, \dots, X_n]$).

Definition 2.2. Let M be an R -module. A subset $N \subseteq M$ is called an $(R\text{-})$ submodule of M if

1. $N \subseteq M$ is a subgroup.
2. For all $\lambda \in R$ and all $x \in N$, $\lambda x \in N$.

Then $\cdot|_{R \times N} : R \times N \rightarrow N$ is an R -module structure on N , i.e. N is an R -module.

Remarks and Examples.

1. Let G be an abelian group and $H \subseteq G$ a subset. Then $H \subseteq G$ is a subgroup iff $H \subseteq G$ is a \mathbb{Z} -submodule.
2. Let $I \subseteq R$ be a subset. Then $I \subseteq R$ is an ideal iff $I \subseteq R$ is an R -submodule.
3. By abuse of notation, we denote by 0 the zero-module $\{0_M\}$. 0 and M are trivially R -submodules of M . M is called *simple* if $0 \neq M$ and $0, M$ are the only submodules of M .
4. If $(M_j)_{j \in J}$ is a family of R -submodules, then $\bigcap_{j \in J} M_j$ and

$$\sum_{j \in J} M_j := \left\{ \sum_{j \in J} m_j \mid m_j \in M_j, m_j = 0 \text{ for almost all } j \in J \right\}$$

are submodules of M . In particular, if $M_1, M_2 \subseteq M$ are submodules, then $M_1 + M_2 = \{m_1 + m_2 \mid m_1 \in M_1, m_2 \in M_2\}$ is a submodule.

Definition 2.3. Let M be an R -module and $E \subseteq M$ a subset. Then

$${}_R\langle E \rangle := \langle E \rangle := \left\{ \sum_{i=1}^n \lambda_i x_i \mid n \in \mathbb{N}, \lambda_1, \dots, \lambda_n \in R, x_1, \dots, x_n \in E \right\} \subseteq M$$

is the *submodule generated by E* .

Remark.

1. It is immediate to check that

$$\langle E \rangle = \bigcap_{\substack{E \subseteq N \subseteq M \\ N \text{ } R\text{-subm.}}} N = \sum_{x \in E} Rx,$$

and therefore $\langle E \rangle$ is the smallest submodule of M containing E .

2. If $E = \{x\}$, then $\langle E \rangle = Rx$.
If $E = \{x_1, \dots, x_n\}$, then $\langle E \rangle = Rx_1 + \dots + Rx_n$.
If $(M_j)_{j \in J}$ is a family of submodules of M , then $\langle \bigcup_{j \in J} M_j \rangle = \sum_{j \in J} M_j$.
3. A subset $E \subseteq M$ is called an *(R -module) generating set of M* if ${}_R\langle E \rangle = M$.
 M is called *finitely generated* if M has a finite generating set. The following considerations are trivial:
 - Suppose R is a field. Then M is a f.g. R -module iff $\dim_R(M) < \infty$.
 - Set $R = \mathbb{Z}$. M is a f.g. \mathbb{Z} -module iff M is a f.g. abelian group.
 - $R[X]$ is not a finitely generated R -module.
4. Let M be a f.g. R -module. Then every generating set contains a finite generating set.

Proof. Let $E \subseteq M$ be a finite generating set and let $E' \subseteq M$ be an arbitrary generating set. So $E \subseteq M = \langle E' \rangle$, and since E is finite there is a finite subset $E'' \subseteq E'$ such that $E \subseteq \langle E'' \rangle$. This implies $M = \langle E \rangle \subseteq \langle \langle E'' \rangle \rangle = \langle E'' \rangle$. \square

Definition 2.4. Let M and N be R -modules. A map $f : M \rightarrow N$ is said to be a *(R -module) homomorphism* if it's a group homomorphism and it's linear, i.e. for all $x, y \in M, \lambda \in R$

- $f(x + y) = f(x) + f(y)$.
- $f(\lambda x) = \lambda f(x)$.

We define $\text{Hom}_R(M, N)$ as the set of all R -homomorphisms $M \rightarrow N$ and $\text{End}_R(M) := \text{Hom}_R(M, M)$, the set of all M -endomorphisms. *Monomorphisms*, *epimorphisms* and *isomorphisms* are defined as injective, surjective and bijective homomorphisms respectively.

Remarks and Examples.

1. Suppose R is a field. Then the R -module homomorphisms are precisely the R -vector space homomorphisms, i.e. the linear maps.
If $R = \mathbb{Z}$, then the \mathbb{Z} -module homomorphisms are precisely the group homomorphisms.
2. Let $M' \subseteq M$ and $N' \subseteq N$ be R -submodules. Let $f \in \text{Hom}_R(M, N)$. We have:
 - (a) $f[M'] \subseteq N$ and $f^{-1}[N'] \subseteq M$ are R -submodules. In particular $\text{Im}(f) := f[M] \subseteq N$ and $\ker(f) := f^{-1}(0) \subseteq M$ are R -submodules.
 - (b) If $f[M'] \subseteq N'$, then $f|_{M'} : M' \rightarrow N'$ is an R -homomorphism. In particular, $f : M \rightarrow f[M]$ is an R -epimorphism.
3. Let $g : M \rightarrow N$ be an R -homomorphism and $E \subseteq M$. We have:
 - (a) $\langle f[E] \rangle = f[\langle E \rangle]$.
 - (b) $f|_E = g|_E \Leftrightarrow f|_{\langle E \rangle} = g|_{\langle E \rangle}$.
4. If $f : M \rightarrow N$ and $g : N \rightarrow P$ are R -homomorphisms, then so is $g \circ f$. If f is an R -isomorphism, then so is f^{-1} .
Notation: we write $M \simeq_R N$ to state that there is an R -isomorphism between M and N .
5. If $f, g \in \text{Hom}_R(M, N)$, then $f + g$ and $-f$ are R -homomorphisms $M \rightarrow N$, where the functions are defined as pointwise sum and inverse. Now observe that

$$\begin{aligned} \alpha f : M &\rightarrow N \\ x &\mapsto \alpha f(x) \end{aligned}$$

is a group homomorphism, for any $\alpha \in R$. Finally, $\lambda(\alpha f) = (\lambda\alpha)f$.

We have just proved the following: $\text{Hom}_R(M, N)$ is an R -module w.r.t. pointwise addition and scalar multiplication $(\alpha, f) \mapsto \alpha f$.

6. Observe that $(\text{End}_R(M), +, \circ) \subseteq (\text{End}_{\mathbb{Z}}(M), +, \circ)$ is a subring, where $1_{\text{End}_R(M)} = \text{id}_M$ (the identity map).

2.1.2 Congruence relations and factor modules.

Definition 2.5. Let M be a non-empty set and \sim an equivalence relation on M .

1. For $a \in M$, let $[a]_\sim := [a] := \{x \in M \mid x \sim a\}$ denote the *equivalence class of a* . We can define the *quotient set* $M/\sim := \{[a] \mid a \in M\}$ and the *canonical projection map*

$$\begin{aligned}\pi_\sim = \pi: M &\rightarrow M/\sim \\ a &\mapsto [a].\end{aligned}$$

2. Suppose that $*$ is a binary operation on M , i.e. $*$: $M \times M \rightarrow M$. Then \sim is called a *congruence relation (w.r.t. $*$)* if, for all $a, a', b, b' \in M$,

$$a \sim a', b \sim b' \Rightarrow a * b \sim a' * b'.$$

Lemma 2.6. Let $(M, *)$ be a semigroup with unit element e and let \sim be a congruence relation on M . Then there is precisely one operation $\tilde{*}$ on M/\sim such that $\pi : M \rightarrow M/\sim$ is a $(*, \tilde{*})$ -epimorphism. In particular:

1. If $(M, *)$ is a group, then so is $(M/\sim, \tilde{*})$.
2. For all $a, b \in M$, we have $[a]\tilde{*}[b] = [a * b]$ and $\ker(\pi) = [e]$ is the unit element of M/\sim .

Proof. Convince yourself that there is nothing to do! □

Definition 2.7. Let M be an R -module. An equivalence relation \sim on M is called a (*R -module*) *congruence relation* if for all $x, x', y, y' \in M$ and $\lambda \in R$:

1. $x \sim x', y \sim y' \Rightarrow x + y \sim x' + y'$.
2. $x \sim x' \Rightarrow \lambda x \sim \lambda x'$.

Remark.

1. Let $N \subseteq M$ be a submodule. For $x, y \in M$ we define $x \equiv_\sim y$ if $x - y \in N$. Then \equiv_\sim is a congruence relation on M .
2. Let \sim be a congruence relation on M and $N := [0]_\sim$. Then $N \subseteq M$ is a submodule and \sim coincides with \equiv_\sim .

Sketch of proof. We know from group theory that $N \subseteq M$ is a subgroup. Let $x \in N, \lambda \in R$. We have to check that $\lambda x \in N$:

$$x \in N \Rightarrow x \sim 0 \Rightarrow \lambda x \sim \lambda 0 = 0 \Rightarrow \lambda x \in N.$$

Clearly, we have that \sim and \equiv_\sim are the same relation. □

Furthermore, $[a]_{\sim} = a + N$, and we define $M/N := M/\sim = \{[a] \mid a \in M\}$.

Lemma 2.8. Let M be an R -module, \sim a congruence relation on M and $N = [0]_{\sim}$. Then there is a uniquely determined R -module structure on M/N such that $\pi_M : M \rightarrow M/N$ is an R -epimorphism. We have that the structure is

$$\begin{aligned} \cdot : R \times M/N &\rightarrow M/N \\ (\lambda, [a]) &\mapsto [\lambda a]. \end{aligned}$$

Proof. Exercise. □

Corollary 2.9. Let M be an R -module, $N \subseteq M$ a submodule and $\pi : M \rightarrow M/N$. Then the maps

$$\begin{aligned} \{N' \subseteq M \mid N \subseteq N' \subseteq M, N' \text{ } R\text{-subm.}\} &\rightarrow \{R\text{-submodules of } M/N\} \\ N' &\mapsto N'/N = \pi[N'] \\ \pi^{-1}[P] &\leftarrow P \end{aligned}$$

are bijections which are inverse to each other.

2.1.3 Isomorphism Theorems for Modules.

Lemma 2.10. Let M and \overline{M} be two non-empty sets. Let $f : M \rightarrow \overline{M}$ and let \sim_f be defined by

$$\forall a, b \in M \quad (a \sim_f b \Leftrightarrow f(a) = f(b)).$$

Then

1. \sim_f is an equivalence relation on M , and for all $a \in M$ we have $[a]_{\sim_f} = f^{-1}[f(a)]$.
2. There is a unique bijection $f^* : M/\sim_f \rightarrow f[M]$ and a unique injection $\overline{f} : M/\sim_f \rightarrow \overline{M}$ such that the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{f} & \overline{M} \\ \pi_{\sim_f} \downarrow & \nearrow \overline{f} & \uparrow \\ M/\sim_f & \xrightarrow{f^*} & f[M] \end{array}$$

i.e. $\overline{f}([a]_{\sim_f}) = f(a)$ and $f^*([a]_{\sim_f}) = f(a)$.

Lemma 2.11 (Abstract homomorphism theorem). Let $f : (M, *) \rightarrow (\overline{M}, \overline{*})$ be a semigroup homomorphism. Then \sim_f is a congruence relation on M , and $f^* : M/\sim_f \rightarrow f[M]$ is a $(\tilde{*}, \overline{*})$ -homomorphism which is bijective, where $\tilde{*}$ is the operation induced by $*$ on M/\sim_f (see Lemma 2.6).

Theorem 2.12 (Homomorphism Theorem for Modules). Let $f : M \rightarrow N$ be an R -module homomorphism, $M' \subseteq M$ and $N' \subseteq N$ be submodules such that $f[M'] \subseteq N'$. Then there is a unique R -homomorphism $f^* : M/M' \rightarrow N/N'$ satisfying

$$f^*(x + M') = f(x) + N' \quad (*)$$

for all $x \in M$. So we have the following commutative diagram:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \pi_M \downarrow & & \downarrow \pi_N \\ M/M' & \xrightarrow{f^*} & N/N' \end{array}$$

Moreover, we have

$$\ker(f^*) = f^{-1}[N']/M' \quad \text{and} \quad \text{Im}(f^*) = (f[M] + N')/N'.$$

As a special case, suppose $M' = \ker(f)$ and $N' = 0$. Then $f^* : M/\ker(f) \rightarrow N$ is an R -monomorphism¹ and thus $M/\ker(f) \simeq f[M]$.

Proof. The uniqueness is trivial, since condition $(*)$ completely determines f^* . We now want to prove the existence, so we have to show that the function f^* defined by $(*)$ is an R -homomorphism. By group theory, we already know that f^* is a group homomorphism. Let $x \in M$ and $\lambda \in R$. We have

$$f^*(\lambda(x + M')) \stackrel{(1)}{=} f^*(\lambda x + M') \stackrel{(2)}{=} f(\lambda x) + N' \stackrel{(3)}{=} \lambda f(x) + N' \stackrel{(4)}{=} \lambda(f(x) + N') \stackrel{(5)}{=} \lambda f^*(x + M'),$$

where (1) and (4) follow by definition of structure on quotient modules (cfr. Lemma 2.8), (2) and (4) are by definition of f^* , and (3) holds because f is an R -module homomorphism by hypothesis.

Clearly, $\ker(f^*)$ and $\text{Im}(f^*)$ have the given form. □

Corollary 2.13 (First isomorphism Theorem for Modules). Let M be an R -module and $A, B \subseteq N$ submodules. Then

$$\begin{aligned} f^* : A/A \cap B &\rightarrow (A + B)/B \\ a + (A \cap B) &\mapsto a + B \end{aligned}$$

is an isomorphism.

¹Of course, we identify N and $N/0$.

Proof. By Theorem 2.12 (with $M := A$, $N := A + B$, $M' := A \cap B$, $N' := B$ and $f := (A \hookrightarrow A + B)$), there is an R -homomorphism

$$f^*: M/M' = A/A \cap B \rightarrow N/N' = (A + B)/B$$

with

$$\ker(f^*) = f^{-1}[B]/A \cap B = (A \cap B)/(A \cap B) = 0$$

and

$$\operatorname{Im}(f^*) = (f[M] + N')/N' = (A + B)/B.$$

□

Corollary 2.14 (Second isomorphism Theorem for Modules). Let M be an R -module and $B \subseteq A \subseteq M$ submodules. Then

$$\begin{aligned} \tilde{f}: (M/B)/(A/B) &\rightarrow M/A \\ (a + B) + (A/B) &\mapsto a + A \end{aligned}$$

is an isomorphism.

Proof. By Theorem 2.12 (with $N := M$, $f := \operatorname{id}_M$, $M' := B$, $N' := A$) there is an R -epimorphism $f^*: M/B \rightarrow M/A$ with $\ker(f^*) = A/B$. □

2.1.4 Between ring and modules.

Definition 2.15. Let M be an R -module.

1. An element $c \in R$ is called a *zero-divisor* on M if there exists $0 \neq x \in M$ s.t. $cx = 0$.
We define $\operatorname{Zdv}_R(M)$ as the set of zero-divisors on M .
 M is called *R -torsionfree* if $\operatorname{Zdv}_R(M) = 0$.
2. Let $E \subseteq M$ be a subset. Then

$$\operatorname{Ann}_R(E) := \{\lambda \in R \mid \lambda x = 0 \text{ for all } x \in E\}$$

is called the *annihilator* of E .

3. M is called *cyclic* if $M = {}_R\langle x \rangle = Rx$ for some $x \in M$.

Remark.

1. For any $E \subseteq M$ we have that $\operatorname{Ann}_R(E) = \operatorname{Ann}_R(\langle E \rangle) = \bigcap_{x \in E} \operatorname{Ann}_R(x) \triangleleft R$ is an ideal of R . Moreover, $\operatorname{Ann}_R(E) = R$ iff $E = \emptyset, \{0\}$.

2. We have $\text{Zdv}_R(M) = \bigcup_{0 \neq x \in M} \text{Ann}_R(x)$. Furthermore

$$M \neq 0 \Leftrightarrow \text{Zdv}_R(M) \neq \emptyset \Leftrightarrow 0 \in \text{Zdv}_R(M).$$

3. If $\pi: M \rightarrow N$ is an R -epimorphism and $M = Rx$ for some $x \in M$, then $N = R\pi(x)$.

Theorem 2.16 (Classification of cyclic R -modules). Let M be an R -module. Then M is cyclic if and only if there exists an ideal $\mathfrak{g} \triangleleft R$ such that $M \simeq R/\mathfrak{g}$.

Proof.

“ \Rightarrow ”: If $M = Rx$ with $x \in M$, then $f: R \rightarrow M$ given by $\lambda \mapsto \lambda x$ is an R -epimorphism with $\ker f = \text{Ann}_R(M) \triangleleft R$.

“ \Leftarrow ”: Since $\pi: R \rightarrow R/\mathfrak{g}$ is an R -epimorphism and $R = R\langle 1 \rangle$, R/\mathfrak{g} is cyclic by point (3) of the remark above. \square

Theorem 2.17. Let M be an R -module. Then

$$\begin{aligned} \varphi: M &\rightarrow \text{Hom}_R(R, M) \\ x &\mapsto (\lambda \mapsto \lambda x) \end{aligned}$$

is an R -isomorphism.

Proof. We will first prove that φ is an R -homomorphism (1), and then we'll show that it is bijective (2).

1. Let $x, x' \in M$. Then, for all $\lambda \in R$,

$$\varphi(x + x')(\lambda) = \lambda(x + x') = \lambda x + \lambda x' = \varphi(x)(\lambda) + \varphi(x')(\lambda) = (\varphi(x) + \varphi(x'))(\lambda)$$

and hence $\varphi(x + x') = \varphi(x) + \varphi(x')$.

Let $x \in M$ and $\mu \in R$. Then, for all $\lambda \in R$,

$$\varphi(\mu x)(\lambda) = \lambda(\mu x) = \mu(\lambda x) = \mu(\varphi(x)(\lambda)) = (\mu\varphi(x))(\lambda)$$

and hence $\varphi(\mu x) = \mu\varphi(x)$.

2. Consider

$$\begin{aligned} \psi: \text{Hom}_R(R, M) &\rightarrow M \\ g &\mapsto g(1). \end{aligned}$$

Then, for all $\lambda \in R$,

$$(\varphi \circ \psi)(g)(\lambda) = \varphi(\psi(g))(\lambda) = \lambda\psi(g) = \lambda g(1) = g(\lambda)$$

and hence $(\varphi \circ \psi)(g) = g$. Furthermore, for all $x \in M$,

$$(\psi \circ \varphi)(x) = \varphi(x)(1) = 1x = x$$

and hence $\varphi \circ \psi = \text{id}_{\text{Hom}_R(R, M)}$ and $\psi \circ \varphi = \text{id}_M$. Therefore φ and ψ are inverse to each other, and we are done. □

Theorem 2.18. Let M be an R -module and $I \triangleleft R$ with $I \subseteq \text{Ann}_R(M)$. Then

1. The function

$$\begin{aligned} R/I \times M &\rightarrow M \\ (\lambda + I, x) &\mapsto \lambda x \end{aligned}$$

is an R/I -module structure on M .

2. If N is an R -module and $I \subseteq \text{Ann}_R(N)$, then

$$\text{Hom}_R(M, N) = \text{Hom}_{R/I}(M, N),$$

where M and N are equipped with the R/I -module structure of point (1).

Proof.

1. If we show that the map is well-defined, then it's easy to check that it is indeed a structure. Let $\lambda, \lambda' \in R$ be s.t. $\lambda + I = \lambda' + I$. We have $\lambda - \lambda' \in \text{Ann}_R(M)$, and thus for all $x \in M$ we get $(\lambda - \lambda')x = 0$, i.e. $\lambda x = \lambda' x$.
2. “ \subseteq ”: Let $f \in \text{Hom}_R(M, N)$. We have to verify that f is R/I -linear. If $\lambda \in R$ and $x \in M$, then

$$f((\lambda + I)x) = f(\lambda x) = \lambda f(x) = (\lambda + I)f(x).$$

“ \supseteq ”: Let $f \in \text{Hom}_{R/I}(M, N)$. We have to verify that f is R -linear. If $\lambda \in R$ and $x \in M$, then

$$f(\lambda x) = f((\lambda + I)x) = (\lambda + I)f(x) = \lambda f(x).$$

□

Examples. Observe that for $R = \mathbb{Z}$, $I = p\mathbb{Z}$, $M = N = (\mathbb{Z}/p\mathbb{Z})^n$, where $n \in \mathbb{N}$, Theorem 2.18 implies that the group homomorphisms (i.e. the \mathbb{Z} -homomorphisms, cfr. first remark at page 13) are the precisely the $\mathbb{Z}/p\mathbb{Z}$ -vector space homomorphisms.

Definition 2.19. Let M be an R -module and $I \triangleleft R$ an ideal. Then

$$IM := \left\{ \sum_{i=1}^k \lambda_i x_i \mid k \in \mathbb{N}, \lambda_1, \dots, \lambda_k \in I, x_1, \dots, x_k \in M \right\}.$$

Remark.

1. $IM \subseteq M$ is an R -submodule.
2. If $M = J \triangleleft R$ then IJ is the usual ideal multiplication.
3. If $J \triangleleft R$, then $(IJ)M = I(JM)$.
4. Since $I \subseteq \text{Ann}_R(M/IM)$, M/IM carries an R/I -module structure by the previous results. In particular, the structure is given by

$$\begin{aligned} \cdot : R/I \times M/IM &\rightarrow M/IM \\ (\lambda + I, x + IM) &\mapsto \lambda x + IM. \end{aligned}$$

2.2 Direct sums, products and free modules.

Definition 2.20. Let $(M_i)_{i \in I}$ be a family of R -modules. Then the generalized Cartesian product $\times_{i \in I} M_i$ (NOTA: aggiungere definizione) is an R -module with component-wise addition and scalar multiplication:

- $(x_i)_{i \in I} + (y_i)_{i \in I} := (x_i + y_i)_{i \in I}$.
- $\lambda \cdot (x_i)_{i \in I} := (\lambda x_i)_{i \in I}$.

We denote $(\times_{i \in I} M_i, +, \cdot)$ by $\prod_{i \in I} M_i$ and we call it *direct product of $(M_i)_{i \in I}$* . Furthermore, we define the *direct sum of $(M_i)_{i \in I}$* as

$$\bigoplus_{i \in I} M_i := \left\{ (x_i)_{i \in I} \in \prod_{i \in I} M_i \mid x_i = 0 \text{ for almost all } i \in I \right\},$$

which is an R -submodule of $\prod_{i \in I} M_i$.

Definition 2.21. For every $j \in I$, we define

$$\begin{aligned} p_j : \prod_{i \in I} M_i &\rightarrow M_j & \text{and} & & \varepsilon_j : M_j &\rightarrow \prod_{i \in I} M_i \\ (x_i)_{i \in I} &\mapsto x_j & & & x_j &\mapsto (\dots, 0, x_j, 0, \dots) \end{aligned}$$

Then p_j is an R -epimorphism (called the *canonical projection*) and ε_j is an R -monomorphism (called the *canonical embedding*).

Special cases:

1. If $M_i = M$ for all $i \in I$, then we trivially have $\prod_{i \in I} M_i = M^I$, and we denote $M^{(I)} := \bigoplus_{i \in I} M_i$.
2. If $I = [1, n]$, then we have

$$\prod_{i \in I} M_i = \prod_{i=1}^n M_i = M_1 \times \dots \times M_n = M_1 \oplus \dots \oplus M_n = \bigoplus_{i=1}^n M_i = \bigoplus_{i \in I} M_i,$$

and if we also have $\forall i \in I (M_i = M)$, then the set above is simply M^n .

Definition 2.22. Let M be an R -module.

1. M is called *free* if $M \simeq R^{(I)}$ for some set I .
2. Let $(M_i)_{i \in I}$ be a family of submodules of M and define

$$g: \bigoplus_{i \in I} M_i \rightarrow M$$

$$(x_i)_{i \in I} \mapsto \sum_{i \in I} x_i.$$

Then g is an R -homomorphism with $\text{Im } g = \sum_{i \in I} M_i$.

We say that $\sum_{i \in I} M_i$ is *direct* if g is an R -monomorphism.

Moreover, M is called (*inner*) *direct sum* of $(M_i)_{i \in I}$ if one of the following equivalent statements is satisfied:

- (a) g is an R -isomorphism.
- (b) $M = \sum_{i \in I} M_i$ and the sum is direct.
- (c) For all $x \in M$ there is a unique tuple $(x_i)_{i \in I} \in \bigoplus_{i \in I} M_i$ such that $x = \sum_{i \in I} x_i$.
- (d) Every $x \in M$ has a unique representation of the form $x = \sum_{i \in I} x_i$ where $x_i \in M_i$ and $x_i = 0$ for almost all $i \in I$.

Observe that if M is inner direct sum of $(M_i)_{i \in I}$, then we can identify M and $\bigoplus_{i \in I} M_i$.

Theorem 2.22. Let M be a module.

1. For any family $(M_i)_{i \in I}$ of R -submodules the following statements are equivalent:
 - (a) The sum of $(M_i)_{i \in I}$ is direct.
 - (b) For all $j \in I$, $M \cap \sum_{i \in I \setminus \{j\}} M_i = 0$.

2. Let $M_1, M_2 \subseteq M$ be submodules. The following are equivalent:

- (a) $M = M_1 + M_2$ and the sum is direct.
- (b) Every $x \in M$ has a unique representation of the form $x = x_1 + x_2$ with $x_1 \in M_1$ and $x_2 \in M_2$.
- (c) $M = M_1 + M_2$ and $M_1 \cap M_2 = 0$.

If these conditions are satisfied, then

$$\begin{array}{ccc} M_1 \rightarrow M/M_2 & \text{and} & M_2 \rightarrow M/M_1 \\ x_1 \mapsto x_1 + M_2 & & x_2 \mapsto x_2 + M_1 \end{array}$$

are isomorphisms.

Proof. Let $g : \bigoplus_{i \in I} M_i \rightarrow M$ be the homomorphism given in Definition 2.22.(2).

1. (a) \Rightarrow (b): By hypothesis, g is injective. Let $j \in I$ and consider an element $z \in M \cap \sum_{i \in I \setminus \{j\}} M_i$. Then $z = \sum_{i \in I \setminus \{j\}} x_i$ for some $x_i \in M_i$ with $x_i = 0$ for almost all $i \in I \setminus \{j\}$. Set $x_j := -z$. We have $g((x_i)_{i \in I}) = 0$, and hence $(x_i)_{i \in I} = 0$, i.e. $z = 0$.
(b) \Rightarrow (a): If $(x_i)_{i \in I} \in \ker g$, then

$$\underbrace{-x_j}_{\in M_j} = \underbrace{\sum_{i \in I \setminus \{j\}} x_i}_{\in \sum_{i \in I \setminus \{j\}} M_i},$$

for all $j \in I$. Thus $x_j \in M_j \cap \sum_{i \in I \setminus \{j\}} M_i$ for all $j \in I$, and so $(x_i)_{i \in I} = 0$, i.e. g is injective.

2. (a) \Leftrightarrow (b): See characterization (d) in Definition 2.22.(2).
(b) \Leftrightarrow (c): This is a particular case of (1).

Finally, by 2(c) it follows that $M_1/(M_1 \cap M_2) = M_1/0 = M_1$ and $(M_1 + M_2)/M_2 = M/M_2$, so the statement follows by the First isomorphism Theorem (Corollary 2.13).

□

Definition 2.23. Let M be an R -module, $(e_i)_{i \in I}$ a family of elements of M and

$$\begin{aligned} g: R^{(I)} &\rightarrow M \\ (\lambda_i)_{i \in I} &\mapsto \sum_{i \in I} \lambda_i e_i. \end{aligned}$$

Observe that g is an R -homomorphism. The family $(e_i)_{i \in I}$ is called

- $(R\text{-})$ linearly independent if g is an R -monomorphism.
- an $(R\text{-})$ basis if g is an R -isomorphism, or equivalently, if:

Every $x \in M$ has a unique representation of the form $x \in \sum_{i \in I} \lambda_i e_i$ with $\lambda_i \in R$ and $\lambda_i = 0$ for almost all $i \in I$,

or, equivalently, if:

$$(e_i)_{i \in I} \text{ is linearly independent and } M = {}_R\langle e_i \mid i \in I \rangle.$$

- A set $B \subseteq M$ is called *linearly independent* (resp. *basis*) if the family $(b)_{b \in B}$ is linearly independent (resp. a basis).

Remark.

1. Consider a ring R as an R -module. Then:
 - $\{1\}$ is an R -basis of R .
 - An element $a \in R$ is l.i. iff $a \notin \text{Zdv}(R)$.
 - If $a, b \in R$, then (a, b) is l.i. in (??? COPIARE).
2. Let I be a set (??? COPIARE)
3. Let R be a domain and let $K := \mathbf{q}(R)$. Then K is a torsionfree R -module and for all $a, b \in K$ the pair $(a, b) \in K \oplus K$ is linearly independent over R .
4. Let $n \in \mathbb{N}_{\geq 2}$. The \mathbb{Z} -module $\mathbb{Z}/n\mathbb{Z}$ has no independent elements, since $n(a + n\mathbb{Z}) = 0$ for all $a \in \mathbb{Z}$, and so it has no basis. Moreover, we have that $\mathbb{Z} = {}_{\mathbb{Z}}\langle 2, 3 \rangle$, i.e. $\{2, 3\}$ is a generating set for \mathbb{Z} as a \mathbb{Z} module.

Theorem 2.24. Let M be an R -module. The following statements hold:

1. M is free iff M has a basis.
2. For a family $(e_i)_{i \in I}$ the following are equivalent:
 - (a) $(e_i)_{i \in I}$ is a basis.
 - (b) $M = \sum_{i \in I} R e_i$, where the sum is direct, and $\text{Ann}_R(e_i) = 0$ for all $i \in I$.
3. If M is free, then $\text{Zdv}_R(M) \subseteq \text{Zdv}_R(R)$. In particular, if R is a domain then every free module is torsionfree.
4. If M is free, then $\text{Ann}_R(M) = 0$.

5. Let B be a basis of M , N an R -module and $f_\circ : B \rightarrow N$ a map. Then there is a unique $f \in \text{Hom}_R(M, N)$ s.t. $f|_B = f_\circ$.

Proof.

1. “ \Rightarrow ”: M is free, i.e. by definition there exists an R -isomorphism $f : R^{(I)} \rightarrow M$. If $(e_i)_{i \in I}$ is the basis of $R^{(I)}$ given in the previous Remark, then $(f(e_i))_{i \in I}$ is a basis of M by Definition 2.23.
“ \Leftarrow ”: By hypothesis

$$\begin{aligned} g : R^{(I)} &\rightarrow M \\ (\lambda_i)_{i \in I} &\mapsto \sum_{i \in I} \lambda_i e_i \end{aligned}$$

is an R -isomorphism. Then M is free by definition.

2. Consider

$$\begin{aligned} g : R^{(I)} &\xrightarrow{\varphi} \bigoplus_{i \in I} Re_i \xrightarrow{\psi} M \\ (\lambda_i)_{i \in I} &\mapsto (\lambda_i e_i)_{i \in I} \mapsto \sum_{i \in I} \lambda_i e_i. \end{aligned}$$

Observe that φ is an R -epimorphism and $\ker \varphi = \bigoplus_{i \in I} \text{Ann}_R(e_i)$. We have:

$(e_i)_{i \in I}$ is a basis $\Leftrightarrow g$ is an isomorphism $\Leftrightarrow \varphi$ and ψ are R -isomorphisms $\Leftrightarrow \text{Ann}_R(e_i) = 0$ for all $i \in I$ and $M = \sum_{i \in I} Re_i$, where the sum is direct.

3. Let $(e_i)_{i \in I}$ be a basis of M and $c \in \text{Zdv}_R(M)$. Then there is a $0 \neq x \in M$ s.t. $cx = 0$. Write $x = \sum_{i \in I} \lambda_i e_i$ with $\lambda_i \in R$. If $j \in I$ is such that $\lambda_j \neq 0$, since

$$0 = cx = \sum_{i \in I} c\lambda_i e_i,$$

we obtain $c\lambda_j = 0$, i.e. $c \in \text{Zdv}_R(R)$.

4. If $(e_i)_{i \in I}$ is a basis of M , then $\text{Ann}_R(M) \subseteq \text{Ann}_R(e_i) = 0$ for any $i \in I$.
5. Every $x \in M$ has a unique representation, therefore $x = \sum_{b \in B} \lambda_b b$ with $\lambda_b \in R$ and $\lambda_b = 0$ for almost all $b \in B$. Then

$$\begin{aligned} f : M &\rightarrow N \\ x &\mapsto \sum_{b \in B} \lambda_b f_\circ(b) \end{aligned}$$

is an R -homomorphism which extends f_\circ . It is trivially the only one.

□

Theorem 2.25. Let $R \neq \{0\}$.

1. R is a field if and only if every R -module is free.
2. R is a PID if and only if every submodule of a free module is free.

Proof.

1. “ \Leftarrow ”: By contraposition: if R is not a field, then there exists $a \in R^\circ \setminus R^\times$, and hence $R/aR \neq 0$, so $\text{Ann}_R(R/aR) = aR \neq 0$. Then Theorem 2.24 implies that R/aR is not free.
“ \Rightarrow ”: Suppose R is a field and let M be an R -module. Consider

$$\Omega := \{B \subseteq M \mid B \text{ is } R\text{-linearly independent}\}.$$

$\Omega \neq \emptyset$, since $\emptyset \in \Omega$. If $\Sigma \subseteq \Omega$ is a chain, then $\bigcup_{B \in \Sigma} B \in \Omega$,² and it's obviously an upper bound for Σ . Therefore Ω has a maximal element B^* by Zorn's Lemma.

Since $B^* \in \Omega$, it is linearly independent, so it is left to show that $\langle B^* \rangle = M$. Assume to the contrary that there exists $z \in M \setminus \langle B^* \rangle$.

Claim: $B^* \cup \{z\}$ is linearly independent.

Proof: Suppose $\lambda z + \sum_{b \in B^*} \lambda_b b = 0$, where $\lambda, \lambda_b \in R$ and almost all $\lambda_b = 0$. If $\lambda \neq 0$, then $z = -\sum_{b \in B^*} \frac{\lambda_b}{\lambda} b \in \langle B^* \rangle$, contradiction. ■

The claim clearly contradicts the maximality of B^* .

2. “ \Leftarrow ”: Since R is free as an R -module (cfr. point (1) of last Remark), by hypothesis every ideal of R is free as an R -module.

Claim: $\text{Zdv}(R) = \{0\}$, i.e. R is a domain.

Proof: Assume to the contrary that there is a $0 \neq \theta \in \text{Zdv}(R)$. Then there is a $c \in R^\circ$ s.t. $c\theta = 0$, i.e. $c \in \text{Ann}_R(\theta R)$ and $\theta R \subseteq R$ is not free by Theorem 2.24.(3), contradiction. ■

Now let $I \triangleleft R$ be an ideal. I must be free, so we consider a basis $(e_i)_{i \in J}$ of I over R . But necessarily $|(e_i)_{i \in J}| = 1$, since $e_i e_j + e_j(-e_i) = 0$. Therefore $I = Re$ for some $e \in I$.³

²This is trivial, but observe that it is basically due to the fact that the definition of linear independency considers only finite subset.

³Observe that we proved the following: if $B \subseteq R$ is an R -linearly independent subset, then $|B| = 1$.

“ \Rightarrow ”: Let M be a free R -module, B a basis of M and $N \subseteq M$ a submodule. Let Ω be the set of all triples (C, C', f) with $C' \subseteq C \subseteq B$ and $f : C' \rightarrow {}_R\langle C \rangle \cap N$ is an homomorphism such that $f[C']$ is a basis of $\langle C \rangle \cap N$. Since $(\emptyset, \emptyset, \emptyset) \in \Omega$, we have that $\Omega \neq \emptyset$. We define the partial order “ \leq ” on Ω in the obvious way⁴

$$(C, C', f) \leq (D, D', g) \stackrel{\text{def}}{\iff} C \subseteq D, C' \subseteq D', f \subseteq g.$$

By considering the union of chains as usual, it is immediate to check that (Ω, \leq) satisfies the assumptions of Zorn’s lemma, and hence it has a maximal element (C, C', f) .

We claim that $C = B$ (then $f[C']$ is a basis of N , and we are done). Assume to the contrary that there is a $u \in B \setminus C$. Define $D := C \cup \{u\}$ and observe that

$$\langle D \rangle = \langle C \rangle + Ru, \text{ where the sum is direct (because } B \text{ is l.i.), and } \langle C \rangle \subsetneq \langle D \rangle.$$

We now have two possible cases:

CASE 1: $\langle D \rangle \cap N = \langle C \rangle \cap N$. Then obviously $f[C']$ is a base of $\langle D \rangle \cap N$ too, and so $(D, C', f) \in \Omega$. But $(D, C', f) > (C, C', f)$, which contradicts the maximality of (C, C', f) .

CASE 2: $\langle D \rangle \cap N \supsetneq \langle C \rangle \cap N$. In particular, this means that there exists $y + \lambda u \in \langle D \rangle \cap N \setminus \langle C \rangle \cap N$, where $y \in \langle C \rangle$ and $\lambda \in R$, i.e. there exists $\lambda \in R$ s.t. $y + \lambda u \in \langle D \rangle \cap N \setminus \langle C \rangle$. We define:

$$\mathfrak{a} := \{\lambda \in R \mid \exists y \in \langle C \rangle \text{ s.t. } y + \lambda u \in N\} \subseteq R.$$

Then $0 \neq \mathfrak{a} \triangleleft R$, and so by hypothesis we have $\mathfrak{a} = aR$ for some $a \in R^\circ$. Choose $x \in \langle C \rangle$ s.t. $x + au \in N$. Now define $D' := C' \cup \{u\}$ and

$$\begin{aligned} g : D' &\rightarrow \langle D \rangle \cap N \\ g|_{C'} &:= f \\ u &\mapsto x + au. \end{aligned}$$

Claim: $g[D']$ is a basis of $\langle D \rangle \cap N$.

Proof: We proceed in two steps:

- (i) $g[D']$ is R -linearly independent.
- (ii) $\langle g[D'] \rangle = \langle D \rangle \cap N$.

⁴Recall that a function is a set of ordered pairs.

In order to show (i), suppose that $\lambda(x+au) + \sum_{y \in f[C']} \lambda_y y = 0$, where $\lambda, \lambda_y \in R$. If $\lambda = 0$, then all $\lambda_y = 0$. If $\lambda \neq 0$, then $(\lambda a)u = -\lambda x - \sum \lambda_y y \in \langle C \rangle$. Since R is a domain, we obtain $\lambda a \neq 0$, which contradicts the assumption $u \in B \setminus C$.

As for (ii), observe that we only have to show the “ \supseteq ” inclusion. Let $z \in \langle D \rangle \cap N$. Since $z \in \langle D \rangle$, then $z = y + cu$ for some $y \in \langle C \rangle$ and $c \in R$. But $z \in N$ too, so $c \in \mathfrak{a} = aR$, i.e. $c = ab$ for some $b \in R$. Then

$$\underbrace{z - b(x + au)}_{\in \langle D \rangle \cap N} = \underbrace{y - bx}_{\in \langle C \rangle} \in \langle C \rangle \cap N = \langle f[C'] \rangle.$$

Hence $z \in \langle f[C'] \rangle + Rg(u) = \langle g[D'] \rangle$. ■

The claim implies that $(D, D', g) \in \Omega$ and $(D, D', g) > (C, C', f)$, which contradicts the maximality of (C, C', f) . □

Theorem 2.26. Let $R \neq \{0\}$. Let M be a free R -module. Suppose that there exists a basis of M which is finite. Then every basis is finite and has the same cardinality. We call this cardinality *rank of M* and we denote it by $\text{rk}(M)$.⁵

Proof. We will use the following two facts:

F1. R has a maximal ideal \mathfrak{m} .

F2. The statement holds for vector spaces (basic Linear Algebra result).

The statement trivially holds if $M = 0$. Suppose that $M \neq 0$. By point (4) of the Remark at page 20, $M/\mathfrak{m}M$ is an R/\mathfrak{m} -module (i.e. an R/\mathfrak{m} -vector space, since R/\mathfrak{m} is a field). Let $(e_i)_{i \in I}$ with $|I| \geq 1$ be a basis of M over R . Then $\{e_i + \mathfrak{m}M \mid i \in I\}$ is an R/\mathfrak{m} -generating set of $M/\mathfrak{m}M$.⁶ It is sufficient to prove that it is also linearly independent over R/\mathfrak{m} (then the assertion follows from F2⁷).

Let $(\lambda_i)_{i \in I}$ be a family of elements of R/\mathfrak{m} , almost all equal to 0, such that

$$\sum_{i \in I} \lambda_i (e_i + \mathfrak{m}M) = 0.$$

⁵Actually the statement we will prove is more general: all the bases of a free R -module have the same cardinality.

⁶The whole argument is the following: $\{e_i + \mathfrak{m}M \mid i \in I\}$ is trivially an R -generating set of $M/\mathfrak{m}M$ (just consider the projection). Therefore it is clearly also an R/\mathfrak{m} -generating set of $M/\mathfrak{m}M$ (see Definition 2.18).

⁷because “ $\{e_i + \mathfrak{m}M \mid i \in I\}$ linearly independent” implies also $|\{e_i + \mathfrak{m}M \mid i \in I\}| = |I| = |(e_i)_{i \in I}|$.

We can write every λ_i as $\lambda_i = r_i + \mathfrak{m}$, for a sequence $(r_i)_{i \in I}$ of elements of R , where $r_i \in \mathfrak{m}$ for almost all $i \in I$. We can assume w.l.o.g. that $r_i = 0$ for almost all $i \in I$. So we obtain

$$0 = \sum_{i \in I} \lambda_i(e_i + \mathfrak{m}M) = \sum_{i \in I} (r_i + \mathfrak{m})(e_i + \mathfrak{m}M) = \sum_{i \in I} r_i e_i + \mathfrak{m}M,$$

i.e.

$$\sum_{i \in I} r_i e_i \in \mathfrak{m}M.$$

So we have $\sum_{i \in I} r_i e_i = \sum_{j=1}^n a_j x_j$ for some $n \in \mathbb{N}, a_j \in \mathfrak{m}, x_j \in M$. Since $(e_i)_{i \in I}$ generates M , we obtain

$$\sum_{i \in I} r_i e_i = \sum_{j=1}^n \left(a_j \sum_{i \in I} q_{i,j} e_i \right)$$

for some $q_{i,j} \in R$, almost all equal to 0. Now observe that

$$\sum_{i \in I} r_i e_i = \sum_{j=1}^n \sum_{i \in I} q_{i,j} a_j e_i = \sum_{i \in I} \sum_{j=1}^n q_{i,j} a_j e_i = \sum_{i \in I} \underbrace{\left(\sum_{j=1}^n q_{i,j} a_j \right)}_{=: b_i} e_i = \sum_{i \in I} b_i e_i,$$

where $b_i := \sum_{j=1}^n q_{i,j} a_j \in \mathfrak{m}$, since \mathfrak{m} is an ideal. Now, because $(e_i)_{i \in I}$ is a basis of M , we get $r_i = b_i$ for all $i \in I$. Thus $\lambda_i = r_i + \mathfrak{m} = b_i + \mathfrak{m} = \mathfrak{m} = 0_{R/\mathfrak{m}}$ for all $i \in I$. \square

Theorem 2.27. Every (finitely generated) R -module is epimorphic image of a (resp. finitely generated) free R -module.

Proof. Let M be an R -module and $E = \{x_i \mid i \in I\} \subseteq M$ a generating set of M . Then $M = \sum_{i \in I} R x_i$, and so

$$\begin{aligned} R^{(I)} &\rightarrow M \\ e_i &:= \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \end{pmatrix} \mapsto x_i \end{aligned}$$

is an R -epimorphism. \square

2.3 Noetherian and Artinian Modules.

Proposition 2.28. Let M be an R -module. The following statements are equivalent:

(a) Every ascending chain of submodules becomes stationary, i.e.

If $M_0 \subseteq M_1 \subseteq \dots$ is an ascending chain of submodules of M , then there is an $m \in \mathbb{N}$ s.t. $M_n = M_m$ for all $n \geq m$.

(b) Every non empty set of submodules of M has a maximal element w.r.t. set-inclusion.

(c) Every submodule is finitely generated.

Proof.

(a) \Rightarrow (b): Assume to the contrary that there is a non-empty set Ω of submodules which has no maximal element, i.e. for all $N \in \Omega$ there is an $N' \in \Omega$ s.t. $N \subsetneq N'$. Choose any $N_0 \in \Omega$ and define recursively a sequence $(N_n)_{n \in \mathbb{N}}$ by $N_{n+1} := N'_n$. Then the chain $N_0 \subsetneq N_1 \subsetneq \dots$ does not become stationary.

(b) \Rightarrow (c): Let $N \subseteq M$ be a submodule. Consider

$$\Omega := \{N' \subseteq N \mid N' \text{ is a finitely generated submodule}\}.$$

Since $0 \in \Omega$, Ω is non-empty and hence it contains a maximal element N^* . Assume towards a contradiction that $N^* \subsetneq N$. If $x \in N \setminus N^*$, then $N^* \subsetneq {}_R\langle N^*, x \rangle \in \Omega$, which contradicts the maximality of N^* . So $N^* = N$, thus N is finitely generated.

(c) \Rightarrow (a): Let $(N_k)_{k \in \mathbb{N}}$ be an ascending chain of submodules. Then $N := \bigcup_{k \in \mathbb{N}} N_k \subseteq M$ is a submodule, and hence $N = {}_R\langle x_1, \dots, x_n \rangle$ for some $x_1, \dots, x_n \in N$. We have that $x_i \in N_{k_i}$ for all $i \in [1, n]$. Define $n := \max\{k_1, \dots, k_n\}$. Then $N = \langle x_1, \dots, x_n \rangle = N_n \subseteq N_{n'} \subseteq N$, for all $n' \geq n$, and we are done. \square

Definition 2.29. Let M be an R -module.

1. M is called *(R-)noetherian* if it satisfies the one of the equivalent statements of Proposition 2.28.
2. R is called a *noetherian ring* if it is a noetherian R -module.

Remark.

1. Every PID is noetherian (since submodules are precisely the ideals, and they are generated by a single element).

2. Every noetherian module is finitely generated.
3. Later we will show that:
 - If R is a field, then M is noetherian iff $\dim_R M < \infty$.
 - If R is noetherian, then $R[X]$ is a noetherian ring.
4. Let R be a domain. Then $R[(X_n)_{n \geq 1}]$ is not a noetherian ring (since $(X_n)_{n \geq 1}$ is linearly independent⁸).
5. Let R be any non-noetherian ring. As we know, $R = {}_R\langle 1 \rangle$ is a free R -module with $\{1\}$ as a basis, but R has submodules which are not finitely generated. In particular, this means that a f.g. module needs not to be noetherian.

Definition 2.30.

1. An R -module M is called *(R -)artinian* if one of the following equivalent (exercise) statements holds:
 - Every descending chain of submodules becomes stationary.
 - Every non-empty set of submodules contains a minimal element w.r.t. set-inclusion.
 - Every factor module is finitely cogenerated, i.e.

If $N \subseteq M$ is a submodule and $(M_i)_{i \in I}$ is a family of submodules of M/N with $\bigcap_{i \in I} M_i = 0$, then there is a finite $J \subseteq I$ s.t. $\bigcap_{j \in J} M_j = 0$.

2. R is called *artinian* if it is an artinian R -module.

Remark.

1. \mathbb{Z} is noetherian, but not artinian (consider the chain $p\mathbb{Z} \supseteq p^2\mathbb{Z} \supseteq p^3\mathbb{Z} \supseteq \dots$ for some $p \in \mathbb{P}$).
2. In an artinian ring, every prime ideal is maximal.

Proof. Let R be artinian and $\mathfrak{p} \triangleleft R$ prime. Then R/\mathfrak{p} is an artinian domain⁹. If $0 \neq x \in R/\mathfrak{p}$, then $\langle x \rangle \supseteq \langle x^2 \rangle \supseteq \langle x^3 \rangle \supseteq \dots$ is a descending chain of submodules. Then there is an $r \in \mathbb{N}$ s.t. $x^r = yx^{r+1}$ for some $y \in R/\mathfrak{p}$. This implies $0 = x^r(xy - 1)$, so $xy = 1$, i.e. $x \in (R/\mathfrak{p})^\times$. Thus R/\mathfrak{p} is a field, i.e. \mathfrak{p} is maximal. \square

⁸Suppose $X_k = \lambda_1 X_{n_1} + \dots + \lambda_r X_{n_r}$, with $n_i \neq k$. Evaluate the polynomial in $\mathbf{e}_k \in R^\mathbb{N}$. We get $1 = 0$, contradiction.

⁹This is easy to check using Corollary 2.9.

Theorem 2.31. Let R be a field and M an R -module. The following are equivalent:

- (a) M is a finite dimensional vector space.
- (b) M is a noetherian R -module.
- (c) M is an artinian R -module.

Proof.

(a) \Rightarrow (b) and (a) \Rightarrow (c): Let $\dim_R M = n$ and let $N \subseteq M$ be a submodule. We use the following facts:

- $\dim_R N \leq \dim_R M$.
- $N = M$ iff $\dim_R N = \dim_R M$.¹⁰

Therefore for any chain of submodules

$$N_0 \subsetneq N_1 \subsetneq \dots \subsetneq N_t \subsetneq \dots \subsetneq M$$

we must have $t \leq \dim_R M$. Thus M is noetherian. M is also artinian by the same argument, with the inverse inclusion.

(b) \Rightarrow (a) and (c) \Rightarrow (a): Assume to the contrary that $\dim_R(M) \geq |\mathbb{N}|$. Then there exist R -linearly independent elements $(u_n)_{n \in \mathbb{N}}$ in M . For every $n \in \mathbb{N}$, define

$$L_n := \sum_{i=1}^n Ru_i \quad \text{and} \quad M_n := \sum_{i=n+1}^{\infty} Ru_i.$$

Then $L_0 \subsetneq L_1 \subsetneq \dots$ and $M_0 \supsetneq M_1 \supsetneq \dots$ are chains which do not become stationary. \square

Definition 2.32.

1. Let L , M and N be R -modules, $\varphi : L \rightarrow M$ and $\psi : M \rightarrow N$ be R -homomorphisms. We say that $L \xrightarrow{\varphi} M \xrightarrow{\psi} N$ is an *exact sequence* (of R -modules) if $\text{Im } \varphi = \ker \psi$.
2. By $0 \rightarrow L$ and $L \rightarrow 0$ we always mean the zero homomorphism. Note that $\text{Im}(0 \rightarrow L) = 0$ and $\ker(L \rightarrow 0) = L$. So:
 - $0 \rightarrow L \xrightarrow{\varphi} M$ is exact iff φ is an R -monomorphism.
 - $M \xrightarrow{\psi} N \rightarrow 0$ is exact iff ψ is an R -epimorphism.

¹⁰Observe that this does not hold for groups: $2\mathbb{Z} \subsetneq \mathbb{Z}$, but $\text{rk}_{\mathbb{Z}}(2\mathbb{Z}) = 1 = \text{rk}_{\mathbb{Z}}(\mathbb{Z})$.

3. A (finite or infinite) sequence of R -homomorphisms

$$\dots \rightarrow M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \rightarrow \dots$$

(where $I \subseteq \mathbb{Z}$ is an interval and the M_i 's are R -modules) is called *exact* if $M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1}$ is exact for all $i \in I$.

An exact sequence of the form

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

is called *short exact sequence*.

Remark. Let $0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \rightarrow 0$ be a short sequence.

1. The sequence is exact iff φ is a monomorphism, ψ is an epimorphism and $\text{Im}(\varphi) = \ker(\psi)$.
2. If the sequence is exact, then
 - φ induces an R -isomorphism $L \rightarrow \varphi[L]$.
 - ψ induces an R -isomorphism $M/\varphi[L] \rightarrow N$.

3. Every R -monomorphism $0 \rightarrow L \xrightarrow{\varphi} M$ induces a short exact sequence:

$$0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\pi} M/\ker(\varphi) \rightarrow 0.$$

4. Every R -epimorphism $M \xrightarrow{\psi} N \rightarrow 0$ induces a short exact sequence:

$$0 \rightarrow \ker(\psi) \hookrightarrow M \xrightarrow{\psi} N \rightarrow 0.$$

The following example is important.

Examples. Let M_1, M_2 be R -modules. Consider the projections

$$\begin{array}{ccc} p_1: M_1 \oplus M_2 \rightarrow M_1 & \text{and} & p_2: M_1 \oplus M_2 \rightarrow M_2 \\ (x_1, x_2) \mapsto x_1 & & (x_1, x_2) \mapsto x_2 \end{array}$$

and the embeddings

$$\begin{array}{ccc} \varepsilon_1: M_1 \rightarrow M_1 \oplus M_2 & \text{and} & \varepsilon_2: M_2 \rightarrow M_1 \oplus M_2 \\ x_1 \mapsto (x_1, 0) & & x_2 \mapsto (0, x_2). \end{array}$$

Of course $p_1 \circ \varepsilon_1 = \text{id}_{M_1}$, $p_2 \circ \varepsilon_2 = \text{id}_{M_2}$, $p_1 \circ \varepsilon_2 = 0$, $p_2 \circ \varepsilon_1 = 0$ and $\varepsilon_1 \circ p_1 + \varepsilon_2 \circ p_2 = \text{id}_{M_1 \oplus M_2}$. Therefore

$$0 \rightarrow M_1 \xrightarrow{\varepsilon_1} M_1 \oplus M_2 \xrightarrow{p_2} M_2 \rightarrow 0$$

and

$$0 \rightarrow M_2 \xrightarrow{\varepsilon_2} M_1 \oplus M_2 \xrightarrow{p_1} M_1 \rightarrow 0$$

are exact sequences, since $\text{Im}(\varepsilon_1) = M_1 \oplus 0 = \ker(p_2)$ and $\text{Im}(\varepsilon_2) = 0 \oplus M_2 = \ker(p_1)$.

Addendum (Splitting lemma). Given a short exact sequence of R -modules,

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

$\nwarrow \text{---} p \text{---} \swarrow$ $\nwarrow \text{---} \varepsilon \text{---} \swarrow$

the following statements are equivalent:

1. There exists an R -homomorphism $p : M \rightarrow L$ such that $p \circ \varphi = \text{id}_L$.
2. There exists an R -homomorphism $\varepsilon : M \rightarrow N$ such that $\psi \circ \varepsilon = \text{id}_N$.
3. There exists an R -isomorphism $f : M \rightarrow L \oplus N$ such that the following diagram commutes:

$$\begin{array}{ccccccc}
 & & & M & & & \\
 & & \nearrow \varphi & & \searrow \psi & & \\
 0 & \longrightarrow & L & & & N & \longrightarrow 0 \\
 & & \searrow \varepsilon_1 & & \nearrow p_2 & & \\
 & & & L \oplus N & & &
 \end{array}$$

$\downarrow f$

Definition 2.33. An exact sequence $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ of R -modules is said to *split* if one of the equivalent statements of the Splitting lemma holds. If the sequence splits, we call it also a *representation of M as a direct sum of L and N* .

Examples. Consider $\{[0], [2]\} \subseteq \mathbb{Z}/4\mathbb{Z}$. The short exact sequence

$$0 \rightarrow \{[0], [2]\} \hookrightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

doesn't split, because $\{[0], [2]\} \simeq \mathbb{Z}/2\mathbb{Z}$, but $\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (since the first is cyclic, the second is not).

Theorem 2.34. Let $0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \rightarrow 0$ be a short exact sequence of R -modules. The following hold:

1. M is noetherian (artinian) if and only if L and N are noetherian (resp. artinian).
2. If L and N are finitely generated, then so is M .

Proof. Since $L \simeq \varphi[L]$ and $M/\varphi[L] \simeq N$, we may assume w.l.o.g. that $L \hookrightarrow M$ is a submodule and $N = M/L$. So the sequence becomes:

$$0 \rightarrow L \hookrightarrow M \xrightarrow{\pi} M/L \rightarrow 0.$$

1. “ \Rightarrow ”: Since M is noetherian (artinian), then $L \subseteq M$ is noetherian (artinian) by definition. If $(J_k)_{k \in \mathbb{N}}$ is an ascending (descending) chain of submodules of M/L , then $J_k = I_k/L$ for all $k \in \mathbb{N}$, where $(I_k)_{k \in \mathbb{N}}$ is an ascending (descending) chain of submodules of M . Since $(I_k)_{k \in \mathbb{N}}$ becomes stationary, the same is true for $(J_k)_{k \in \mathbb{N}}$. So also M/L is noetherian (artinian).

“ \Leftarrow ”: Let $(I_k)_{k \in \mathbb{N}}$ be an ascending chain of submodules of M . Then $(L \cap I_k)_{k \in \mathbb{N}}$ is an ascending chain of submodules of L , and hence there is a $k'' \in \mathbb{N}$ such that $L \cap I_j = L \cap I_{k''}$ for all $j \geq k''$.

Similarly, $(I_k/L)_{k \in \mathbb{N}}$ is an ascending chain of submodules of M/L , and hence there is a $k' \in \mathbb{N}$ such that $I_j/L = I_{k'}/L$ for all $j \geq k'$.

Claim: $I_j = I_k$ for all $j \geq k := \max\{k', k''\}$.

Proof: Suppose $j \geq k$. Then $I_k \subseteq I_j$. We have to show that $I_j \subseteq I_k$. Let $x \in I_j$. Then $\pi(x) = x + L \in I_j/L = I_{k'}/L$. So $x = a + b$ for some $a \in L$, $b \in I_{k'}$. Thus $a = x - b \in L \cap I_j = L \cap I_k \subseteq I_k$, which implies $x = a + b \in I_k$. ■

So M is noetherian.

For artinian modules, the proof runs along the same lines.

2. Let $L = {}_R\langle y_1, \dots, y_m \rangle$ and $M/L = {}_R\langle z_1 + L, \dots, z_n + L \rangle$. We claim that $M = {}_R\langle y_1, \dots, y_m, z_1, \dots, z_n \rangle$.
Let $x \in M$. Then there are $\lambda_1, \dots, \lambda_n \in R$ s.t.

$$x + L = \lambda_1(z_1 + L) + \dots + \lambda_n(z_n + L).$$

Then $x = \sum_{i=1}^n \lambda_i z_i + y$, with $y \in L$. Since $y = \sum_{j=1}^m \mu_j y_j$ for some $\mu_j \in R$, the claim follows, and we are done.

□

Corollary 2.35. Let $n \in \mathbb{N}$ and M_1, \dots, M_n be R -modules. The following are equivalent:

- $M_1 \oplus \dots \oplus M_n$ is noetherian (artinian).
- M_1, \dots, M_n are noetherian (artinian).

Proof. By induction. If $n = 1$ there is nothing to prove. Suppose now $n \geq 2$. There is an exact sequence

$$0 \rightarrow M_1 \hookrightarrow \bigoplus_{i=1}^n M_i \rightarrow \bigoplus_{i=2}^n M_i \rightarrow 0$$

and hence by induction hypothesis the assertion follows from Theorem 2.34. □

Corollary 2.36. The following statements are equivalent:

- (a) R is noetherian (artinian).
- (b) Every finitely generated R -module is noetherian (artinian).

Proof.

(b) \Rightarrow (a): Immediate, since $R = \langle 1 \rangle$ is a f.g. R -module.

(a) \Rightarrow (b): Let M be a f.g. R -module. By Theorem 2.27 there is an $n \in \mathbb{N}$ and an R -epimorphism $\psi : R^n \rightarrow M$. By Corollary 2.35 R^n is noetherian. Since

$$0 \rightarrow \ker \psi \hookrightarrow R^n \xrightarrow{\psi} M \rightarrow 0$$

is exact, M is noetherian by Theorem 2.34. \square

Corollary 2.37. Let R and S be commutative rings, and let $f : R \rightarrow S$ be a ring epimorphism. If R is a noetherian (artinian) ring, then so is S .

Proof. Since $S \simeq R/\ker f$ (as rings), it is sufficient to consider the factor ring R/I , where $I = \ker f$. By hypothesis, R is a noetherian (artinian) R -module, and hence $R/I = {}_R\langle 1 + I \rangle$ is a noetherian (artinian) R -module by Corollary 2.36.

Now consider an ascending (descending) chain of R/I -submodules of R/I . Observe that any R/I -module is trivially also an R -module¹¹. So we can see the chain as an ascending (descending) chain of R -submodules of R/I . Since R/I is a noetherian (artinian) R -module, such chain must stabilize. So R/I is a noetherian (artinian) R/I -module. \square

2.4 Modules of finite length.

Definition 2.38. Let M be an R -module.

1. M is called *simple (over R)* if $M \neq 0$, and 0 and M are the only submodules of M .
2. By $l(M) := l_R(M) \in \mathbb{N} \cup \{\infty\}$ we denote the supremum over all the $l \in \mathbb{N}$ which have the following property: there exists a sequence of submodules

$$M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_l = 0.$$

¹¹Just consider the R -module structure given by $(\lambda, x) \mapsto [\lambda]x$.

3. Let

$$M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_l = 0 \quad (*)$$

be a sequence of submodules. We call $(*)$ a *composition series of length l* if M_{i-1}/M_i is simple for all $i \in [1, l]$ (equivalently, if for all $i \in [1, l]$ there is no module M' s.t. $M_{i-1} \supsetneq M' \supsetneq M_i$).

4. Let

$$M = M'_0 \supsetneq M'_1 \supsetneq \dots \supsetneq M'_k = 0 \quad (**)$$

be another sequence of submodules. We say that

- $(*)$ and $(**)$ are *equivalent* if $k = l$ and there is a permutation $\sigma \in S_l$ such that $M_{i-1}/M_i \simeq M'_{\sigma(i)-1}/M'_{\sigma(i)}$ for all $i \in [1, l]$.
- $(**)$ is a *refinement of $(*)$* if all the M_1, \dots, M_l show up among the M'_1, \dots, M'_k .

Remarks and Examples.

1. Trivially:

- $l(M) = 0 \Leftrightarrow M = 0$.
- $l(M) = 1 \Leftrightarrow M$ is simple.
- $l(M) < \infty \Rightarrow M$ is finitely generated.
- M is finite $\Rightarrow l(M) < \infty$.
- If R is a field, then $l(M) = \dim_R(M)$.

2. Let $R = \mathbb{Z}$. Then $l(M) < \infty \Leftrightarrow M$ is finite.

Proof. “ \Leftarrow ” always holds. As for “ \Rightarrow ”, first observe that M is finitely generated, since $l(M) < \infty$. Furthermore, every element x has finite torsion, because otherwise $\langle x \rangle \simeq \mathbb{Z}$, and so $l(M) \geq l(\langle x \rangle) = l(\mathbb{Z}) = \infty$, against the hypothesis. So M is a finitely generated torsion group, hence it's finite. \square

3. M is simple if and only if $M \simeq R/\mathfrak{m}$ for some $\mathfrak{m} \in \max(R)$.

Proof.

“ \Rightarrow ”: Let $0 \neq x \in M$. Then $0 \neq Rx \subseteq M$ is a submodule, and hence $M = Rx$ because M is simple. But $R/\text{Ann}_R(x) \simeq Rx$ (see proof of Theorem 2.16). Since M is simple, this means that

$$\{0, R/\text{Ann}_R(x)\} = \{R\text{-subm. of } R/\text{Ann}_R(x)\} = \{\mathfrak{g}/\text{Ann}_R(x) \mid \text{Ann}_R(x) \subseteq \mathfrak{g} \triangleleft R\},$$

i.e. $\text{Ann}_R(x) \in \max(R)$.

“ \Leftarrow ”: R/\mathfrak{m} is a field, so its ideals (which are precisely its submodules) are just 0 and itself. \square

4. Let $R = \mathbb{Z}$. By the last point we get that M is simple $\Leftrightarrow M \simeq \mathbb{Z}/p\mathbb{Z}$ for some $p \in \mathbb{P}$.

2.4.1 A parenthesis on lattices.

Let (M, \leq) be a partially ordered set. We give the following definitions:

1. Let $\emptyset \neq T \subseteq M$ be a non-empty subset. Then $a \in M$ is called *supremum* of T if

- $x \leq a$ for all $x \in T$.
- If $e \in M$ and $x \leq e$ for all $x \in T$, then $a \leq e$.

It is immediate to check that if such an a exists, then it is unique. So we can define $\sup T$ as the supremum of T , if it exists. The *infimum* is defined as the supremum w.r.t. the inverse order (M, \geq) .

2. (M, \leq) is called a *lattice* if for every two elements $a, b \in M$, $\sup(a, b)$ and $\inf(a, b)$ exist.
3. A non-empty set M with two binary operations \vee (the *join*) and \wedge (the *meet*) is called a *lattice* if for all $a, b, c \in M$ the following properties are satisfied:

- c1) $a \vee a = a, a \wedge a = a$.
- c2) $a \vee b = b \vee a, a \wedge b = b \wedge a$.
- c3) $(a \vee b) \vee c = a \vee (b \vee c), (a \wedge b) \wedge c = a \wedge (b \wedge c)$.
- c4) $a \wedge (a \vee b) = a, a \vee (a \wedge b) = a$.

The following result is easy to check:

Theorem.

1. If (M, \leq) is a lattice in the sense of (b), then the operations $a \wedge b := \inf(a, b)$ and $a \vee b := \sup(a, b)$ satisfy (c1)–(c4).
2. If (M, \vee, \wedge) is a lattice in the sense of (c), then defining

$$a \leq b \stackrel{\text{def}}{\iff} a \vee b = b$$

we obtain that (M, \leq) is a lattice in the sense of (b).

Definition. A lattice (M, \leq) is called

- *modular*, if for all $a, b, c \in M$ we have

$$c \leq a \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

(which can be proven equivalent to the condition $a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$).

- *distributive*, if for all $a, b, c \in M$ we have

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

(which can be proven equivalent to the condition $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$).

Obviously, any distributive lattice is modular.

Examples.

1. If M is a set, then $(\mathcal{P}(M), \subseteq)$ is a distributive lattice. *Stone's representation theorem for distributive lattices* provides a converse: every distributive lattice is isomorphic to a lattice of set, i.e. to a sublattice of some $(\mathcal{P}(X), \subseteq)$.
2. Let H be a monoid. Then $(H, |)$ is a partially ordered set, where $|$ is the divisibility relation. If H is reduced (i.e. $H^\times = \{1\}$), we have that $|\gcd(A)| \leq 1$ for all $A \subseteq H$ (cfr. Lemma 1.2). It is immediate to check that if $a, b \in H$ are such that $\gcd(a, b) = \{c\}$, then $c = \inf(a, b)$ w.r.t. the divisibility order. So H is a GCD-monoid if and only if $(H, |)$ is a lattice.
3. Let M be an R -module. Then

$$\mathcal{A} := (\{N \subseteq M \mid N \text{ subm.}\}, \subseteq)$$

is a modular lattice, and $\sup(N_1, N_2) = N_1 + N_2$, $\inf(N_1, N_2) = N_1 \cap N_2$. In particular,

$$\mathcal{I} := (\{I \subseteq R \mid I \text{ ideal}\}, \subseteq)$$

is modular.

Proof. Everything is easy to check, so we prove just the modularity. We must show that, for any $A, B, C \in \mathcal{A}$,

$$A \subseteq C \Rightarrow A + (B \cap C) = (A + B) \cap \underbrace{(A + C)}_{=C}.$$

The inclusion “ \subseteq ” is trivial. As for “ \supseteq ”, let $x = a + b \in C$ where $a \in A$ and $b \in B$. Then $b = x - a \in C + A \subseteq C + C = C$, and hence $x = a + b \in A + (B \cap C)$. \square

2.4.2 The Jordan-Hölder Theorem.

Theorem 2.39 (Schreier Refinement Lemma). Let M be an R -module. Each two finite sequences of submodules have two respective refinements which are equivalent.

Proof. Let $M = P_0 \supseteq \dots \supseteq P_r = 0$ and $M = Q_0 \supseteq \dots \supseteq Q_s = 0$ be two sequences of submodules. For all $i \in [1, r]$ and $j \in [1, s]$ define

$$P_{i,j} := P_i + (P_{i-1} \cap Q_j) \quad \text{and} \quad Q_{j,i} := Q_j + (Q_{j-1} \cap P_i).$$

Then we have

$$P_i = P_{i,s} \subseteq P_{i,s-1} \subseteq \dots \subseteq P_{i,0} = P_{i-1}$$

and

$$Q_j = Q_{j,r} \subseteq Q_{j,r-1} \subseteq \dots \subseteq Q_{j,0} = Q_{j-1}.$$

Then the sequence $(P_{i,j})$ is a refinement of (P_i) , and $(Q_{j,i})$ is a refinement of (Q_j) . It is left to show that the sequences $(P_{i,j})$ and $(Q_{i,j})$ are equivalent. Indeed, for all $i \in [1, r]$ and $j \in [1, s]$ we have

$$\begin{aligned} P_{i,j-1}/P_{i,j} &= \frac{P_i + (P_{i-1} \cap Q_{j-1})}{P_i + (P_{i-1} \cap Q_j)} \\ &= \frac{[P_i + (P_{i-1} \cap Q_j)] + (P_{i-1} \cap Q_{j-1})}{[P_i + (P_{i-1} \cap Q_j)]} \\ &\simeq \frac{P_{i-1} \cap Q_{j-1}}{[P_i + (P_{i-1} \cap Q_j)] \cap P_{i-1} \cap Q_{j-1}} \quad (*) \\ &= \frac{P_{i-1} \cap Q_{j-1}}{[P_i + (P_{i-1} \cap Q_j)] \cap Q_{j-1}} \\ &= \frac{P_{i-1} \cap Q_{j-1}}{(P_{i-1} \cap Q_j) + (P_i \cap Q_{j-1})}, \quad (**) \end{aligned}$$

where $(*)$ follows by the First isomorphism Theorem and $(**)$ holds by modularity. In a similar way we can show that

$$Q_{j,i-1}/Q_{j,i} \simeq (Q_{j-1} \cap P_{i-1})/((Q_{j-1} \cap P_i) + (Q_i \cap P_{i-1})),$$

therefore $P_{i,j-1}/P_{i,j} \simeq Q_{j,i-1}/Q_{j,i}$. □

Theorem 2.40 (Jordan-Hölder). Let M be an R -module having a composition series. Then every sequence of submodules can be refined to a composition series, and each two composition series are equivalent (in particular, they have the same length).

Proof. Let

$$M = P_0 \subsetneq \dots \subsetneq P_r = 0 \quad (*)$$

be a sequence of submodules, and

$$M = Q_0 \subsetneq \dots \subsetneq Q_j \quad (**)$$

be a composition series of M . By Theorem 2.39, both sequences $(*)$ and $(**)$ have refinements which are equivalent to each other. However, a composition series can only be refined by repeating some modules (trivial). This gives us a sequence where factor modules are either zero or simple. Then this must also hold for the refinement of $(*)$. Cancelling the unnecessary submodules in both refinements, we obtain a composition $(*)'$ which is a refinement of $(*)$, and obviously we get back (a series equivalent to) $(**)$. Having cancelled only those submodules which lead to zero factor modules, we see that $(*)'$ and $(**)$ are equivalent. \square

Addendum. Observe that in Theorem 2.40 we have also proved that if M has a composition series of length l , then $l(M) = l$.

Theorem 2.41. Let M be an R -module. Then the following facts are equivalent:

1. M has a composition series.
2. $l(M) < \infty$.
3. M is noetherian and artinian.

Proof.

(1) \Rightarrow (2): Follows by last Addendum.

(2) \Rightarrow (3): Since every ascending/descending sequence of submodule contains at most $l(M)$ different submodules not equal to 0, then every such sequence becomes stationary.

(3) \Rightarrow (1): Consider

$$\Omega_1 := \{N \subseteq M \mid N \text{ has a composition series}\}.$$

Since $0 \in \Omega_1$, Ω_1 has a maximal element M_1 . If $M_1 = M$, then we are done. Assume towards a contradiction $M_1 \subsetneq M$. Then

$$\Omega_2 := \{N \subseteq M \mid M_1 \subsetneq N \subseteq M\} \neq \emptyset.$$

Since M is artinian, Ω_2 has a minimal element M_2 . By minimality, we have

$$\nexists N \text{ s.t. } M_2 \supsetneq N \supsetneq M_1.$$

Thus, since M_1 has a composition series, adding M_2 at the beginning we obtain a composition series for M_2 . This contradicts the maximality of M_1 . \square

Theorem 2.42. Let $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ be a short exact sequence. Then $l(M) = l(L) + l(N)$.

Proof. Suppose w.l.o.g. $L \subseteq M$ and $N = M/L$. By Theorem 2.34, M is noetherian and artinian iff L and M/L are noetherian and artinian. Thus by Theorem 2.41 we get

$$l(M) < \infty \iff (l(L) < \infty \text{ and } l(M/L) < \infty).$$

So, if $l(M) = \infty$ the statement follows immediately. Let $l(M) < \infty$ and let

$$L = L_0 \supsetneq \dots \supsetneq L_l = 0$$

and

$$M/L = \tilde{M}_0 \supsetneq \dots \supsetneq \tilde{M}_k = 0$$

be composition series. For $i \in [0, k]$ let $M_i := \pi^{-1}[\tilde{M}_i]$, so that $\tilde{M}_i = M_i/L$. We obtain a sequence of submodules of M

$$M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_k = L \supsetneq L_1 \supsetneq \dots \supsetneq L_l = 0. \quad (*)$$

Since $\tilde{M}_{i-1}/\tilde{M}_i = (M_{i-1}/L)/(M_i/L) \simeq M_{i-1}/M_i$ for all $i \in [1, k]$, the sequence in $(*)$ is a composition series of length $k + l = l(L) + l(M/L)$. \square

2.4.3 Preparation for the Theorem of Krull-Schmidt.

Definition 2.43. An R -module M is called *indecomposable* if $M \neq 0$ and for all submodules $M_1, M_2 \subseteq M$ s.t. $M = M_1 \oplus M_2$, we have $M_1 = 0$ or $M_2 = 0$.

Remark.

1. If R is a field, then M is indecomposable iff $\dim_R(M) = 1$.
2. Let R be a domain and $0 \neq I \triangleleft R$. Then I is indecomposable. Indeed, suppose $I = I_1 \oplus I_2$. If there exist $0 \neq a_j \in I_j$ for $j = 1, 2$, then $0 \neq a_1 a_2 \in I_1 I_2 \subseteq I_1 \cap I_2 = 0$, contradiction.

Theorem 2.44. Let M be a noetherian or artinian R -module. Then there exist indecomposable modules M_1, \dots, M_n with $M = M_1 \oplus \dots \oplus M_n$.

Proof. If $M = 0$, then the statement is trivially true. Let $M \neq 0$. By contraposition, suppose M has no such decomposition. Then M is not decomposable, i.e. $M = M_1 \oplus M'_1$ for some $M_1, M'_1 \neq 0$ and M_1 has no decomposition in indecomposable modules.

By induction, we can re-iterate the process and find, for any $n \geq 1$, a decomposition

$$M = \underbrace{M_n \oplus M'_n \oplus M'_{n-1} \oplus \dots \oplus M'_1}_{M_1}$$

for some $M_n, \dots, M'_n \neq 0$ and $M_n \neq 0$ has no decomposition in indecomposable modules. So we can construct two chains

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \dots \quad \text{and} \quad 0 \subsetneq M'_1 \subsetneq M'_1 \oplus M'_2 \subsetneq \dots,$$

therefore M is not noetherian nor artinian. \square

Remark. In general, there are many such decompositions. Our goal is now to show uniqueness results under certain assumptions.

Theorem 2.45 (Fitting Lemma). Let M be an R -module and $\varphi \in \text{End}_R(M)$. Then:

1. If M is artinian then there is an $n \in \mathbb{N}$ such that

$$M = \text{Im}(\varphi^m) + \ker(\varphi^m) \quad \text{for all } m \geq n.$$

Particularly, φ is bijective $\Leftrightarrow \varphi$ is injective.

2. If M is noetherian, then there is an $n \in \mathbb{N}$ such that

$$\text{Im}(\varphi^m) \cap \ker(\varphi^m) = 0 \quad \text{for all } m \geq n.$$

Particularly, φ is bijective $\Leftrightarrow \varphi$ is surjective.

3. If M is of finite length, then there is an $n \in \mathbb{N}$ such that

$$M = \text{Im}(\varphi^m) \oplus \ker(\varphi^m) \quad \text{for all } m \geq n.$$

Particularly, φ is injective $\Leftrightarrow \varphi$ is surjective.

Proof.

1. The descending chain $M \supseteq \text{Im}(\varphi) \supseteq \text{Im}(\varphi^2) \supseteq \dots$ terminates. Thus there is an $n \in \mathbb{N}$ s.t. $\text{Im}(\varphi^m) = \text{Im}(\varphi^n)$ for all $m \geq n$. Hence for all $m \geq n$ and for all $x \in M$ we have $\varphi^m(x) \in \text{Im}(\varphi^m) = \text{Im}(\varphi^n)$, whereby there is an $y \in M$ s.t. $\varphi^m(x) = \varphi^{2m}(y)$, i.e. $\varphi^m(x - \varphi^m(y)) = 0$. Therefore

$$x = \varphi^m(y) + (x - \varphi^m(y)) \in \text{Im}(\varphi^m) + \ker(\varphi^m).$$

The last statement follows immediately, since $\text{Im}(\varphi) \supseteq \text{Im}(\varphi^m)$, and φ injective implies φ^m injective.

2. The ascending chain $0 \subseteq \ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \dots$ terminates. Thus there is an $n \in \mathbb{N}$ s.t. $\ker(\varphi^m) = \ker(\varphi^n)$ for all $m \geq n$. Observe that $x \in \text{Im}(\varphi^m) \cap \ker(\varphi^m)$ means that there is $y \in M$ s.t. $x = \varphi^m(y)$ and $0 = \varphi^m(x) = \varphi^{2m}(y)$. So, if $m \geq n$ we have $y \in \ker(\varphi^{2m}) = \ker(\varphi^m)$, and we get $x = \varphi^m(y) = 0$.

The last statement follows immediately, since $\ker(\varphi) \subseteq \ker(\varphi^m)$, and φ surjective implies φ^m surjective.

3. Thanks to Theorem 2.41, this is a direct consequence of (1) and (2). □

Definition 2.46. A (not necessarily commutative) ring is called *local* if $R \neq 0$ and one of the following equivalent conditions hold:

1. The sum of non-units is a non-unit.
2. The set of non-units is a two sided ideal.

Proof of the equivalence. The implication “(2) \Leftarrow (1)” is clear. To show “(1) \Rightarrow (2)”, first recall the following easy facts:

- If $x \in R$ has a left and a right inverse, then $x \in R^\times$ (indeed $yx = 1 = xz \Rightarrow y = y1 = y(xz) = (yx)z = z$).
- If $x \in R \setminus R^\times$, then $x^2 \in R \setminus R^\times$ (indeed $x^2 \in R^\times$ would imply that x has a left and right inverse).

We proceed by contraposition. By hypothesis there are $x \in R \setminus R^\times$ and $\lambda \in R$ such that $\lambda x \in R^\times$ or $x\lambda \in R^\times$. Suppose the first case holds, the proof in the other case being similar. If $\lambda \in R^\times$, then $x = \lambda^{-1}(\lambda x) \in R^\times$, contradiction. Thus $\lambda \in R \setminus R^\times$. If $x\lambda \in R^\times$, then x trivially has a left and a right inverse, i.e. $x \in R^\times$, contradiction. Thus $x\lambda \in R \setminus R^\times$. Therefore $R^\times \ni \lambda x = (x + \lambda)^2 - x^2 - x\lambda - \lambda^2$ is a sum of non-units. □

Theorem 2.47. Let M be an indecomposable R -module of finite length. Then the following hold:

1. The non-invertible elements of $\text{End}_R(M)$ are nilpotent.
2. $\text{End}_R(M)$ is a local ring.

Proof.

1. Let $\varphi \in \text{End}_R(M)$ be non-invertible (i.e. not bijective). By Theorem 2.45.(3) there is an $n \in \mathbb{N}$ with $M = \text{Im}(\varphi^n) \oplus \ker(\varphi^n)$. Since M is indecomposable, one summand is 0 and the other is M . If $M = \text{Im}(\varphi^n)$, then φ is surjective and thus bijective, contradiction. Thus $M = \ker(\varphi^n)$, i.e. $\varphi^n = 0$, so φ is nilpotent.
2. We will show that the sum of two non-invertible $\varphi, \psi \in \text{End}_R(M)$ is non-invertible. Suppose to the contrary that there is $\alpha \in \text{End}_R(M)$ such that

$\alpha \circ (\varphi + \psi) = \text{id}_M$. Since $\alpha \circ \varphi$ and $\alpha \circ \psi$ are not invertible, they are nilpotent by first point, i.e. there is an $n \in \mathbb{N}$ such that

$$(\alpha \circ \varphi)^n = 0 = (\alpha \circ \psi)^n.$$

Since $\alpha \circ \varphi$ and $\alpha \circ \psi = \text{id}_M - (\alpha \circ \varphi)$ commute¹², by the binomial theorem we get

$$\text{id}_M = (\text{id}_M)^{2n} = (\alpha \circ \varphi + \alpha \circ \psi)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} (\alpha \circ \varphi)^i \circ (\alpha \circ \psi)^{2n-i} = 0,$$

contradiction.

□

Remark. Given M_1, M_2, N_1, N_2 R -modules, an R -linear map $\varphi : M_1 \oplus M_2 \rightarrow N_1 \oplus N_2$ can be written as

$$\varphi = \begin{pmatrix} \varphi_{1,1} & \varphi_{1,2} \\ \varphi_{2,1} & \varphi_{2,2} \end{pmatrix}$$

with $\varphi_{i,j} : M_j \rightarrow N_i$ R -linear, so that we have

$$\varphi(x_1, x_2) = (y_1, y_2) \iff \begin{cases} \varphi_{1,1}(x_1) + \varphi_{1,2}(x_2) = y_1, \\ \varphi_{2,1}(x_1) + \varphi_{2,2}(x_2) = y_2. \end{cases}$$

This notation is compatible with composition of maps (from and to further direct summands of R -modules).

Lemma 2.48. If φ and $\varphi_{1,1}$ are bijective, then $M_2 \simeq N_2$.

Proof. It is immediate to check that the maps

$$\alpha = \begin{pmatrix} \text{id}_{N_1} & 0 \\ -\varphi_{2,1} \circ \varphi_{1,1}^{-1} & \text{id}_{N_2} \end{pmatrix} : N_1 \oplus N_2 \rightarrow N_1 \oplus N_2$$

and

$$\beta = \begin{pmatrix} \text{id}_{M_1} & -\varphi_{1,1}^{-1} \circ \varphi_{1,2} \\ 0 & \text{id}_{M_2} \end{pmatrix} : M_1 \oplus M_2 \rightarrow M_1 \oplus M_2$$

¹²We need this to apply the Binomial theorem, but it's immediate to check: if $a = 1 - b$, then $ab = b - b^2 = ba$.

are bijective, and thus $\alpha \circ \varphi \circ \beta : M_1 \oplus M_2 \rightarrow N_1 \oplus N_2$ is an isomorphism. We have

$$\begin{aligned} \alpha \circ \varphi \circ \beta &= \begin{pmatrix} \text{id}_{M_1} & 0 \\ -\varphi_{2,1} \circ \varphi_{1,1}^{-1} & \text{id}_{N_2} \end{pmatrix} \circ \begin{pmatrix} \varphi_{1,1} & \varphi_{1,2} \\ \varphi_{2,1} & \varphi_{2,2} \end{pmatrix} \circ \begin{pmatrix} \text{id}_{M_1} & -\varphi_{1,1}^{-1} \circ \varphi_{1,2} \\ 0 & \text{id}_{M_2} \end{pmatrix} \\ &= \begin{pmatrix} \varphi_{1,1} & \varphi_{1,2} \\ 0 & \varphi'_{2,2} \end{pmatrix} \circ \begin{pmatrix} \text{id}_{M_1} & -\varphi_{1,1}^{-1} \circ \varphi_{1,2} \\ 0 & \text{id}_{M_2} \end{pmatrix} \\ &= \begin{pmatrix} \varphi_{1,1} & 0 \\ 0 & \varphi'_{2,2} \end{pmatrix}, \end{aligned}$$

and thus $\varphi'_{2,2} : M_2 \rightarrow N_2$ is an R -isomorphism. \square

Proposition 2.49.

1. Let $M_1, M_2, N_1, \dots, N_s$ be R -modules with $\text{End}_R(M_1)$ local and N_1, \dots, N_s indecomposable. If $M_1 \oplus M_2 \simeq N_1 \oplus \dots \oplus N_s$, then there is an $i \in [1, s]$ such that

$$M_1 \simeq N_i \quad \text{and} \quad M_2 \simeq \bigoplus_{\substack{j=1 \\ j \neq i}}^s N_j.$$

2. Let $M_1, \dots, M_r, N_1, \dots, N_s$ be R -modules with $\text{End}_R(M_1), \dots, \text{End}_R(M_r)$ local and N_1, \dots, N_s indecomposable¹³. If

$$M_1 \oplus \dots \oplus M_r \simeq N_1 \oplus \dots \oplus N_s,$$

then $r = s$ and $M_i \simeq N_{\sigma(i)}$ for some permutation $\sigma \in S_r$, for all $i \in [1, r]$.

Before presenting the proof, we show the main consequence of this theorem. Let \mathcal{C} be a class of R -modules, closed under R -isomorphisms, finite direct sum and direct summands (e.g. noetherian modules, artinian modules, modules of finite length). For a module M , let $[M]$ be the isomorphism class of M . We assume that $\mathcal{V}(\mathcal{C}) = \{[M] \mid M \in \mathcal{C}\}$ is a set. Then $(\mathcal{V}(\mathcal{C}), +)$ is an abelian semigroup with $[M] + [N] := [M \oplus N]$.

Theorem 2.50 (Krull-Schmidt).

1. Let \mathcal{C} be a class of noetherian modules with the above properties. If $\text{End}_R(M)$ is local for all indecomposable $M \in \mathcal{C}$, then $\mathcal{V}(\mathcal{C})$ is factorial.

¹³Observe that by Definition 2.46(2), a local ring trivially has no non-trivial idempotent elements. By Exercise 27, this means that if $\text{End}_R(M)$ is local, then M is indecomposable. The converse doesn't necessarily hold, and indeed an R -module s.t. $\text{End}_R(M)$ is local is sometimes called *strongly indecomposable*. It can be shown that the statement doesn't necessarily hold if we just assume M_1, \dots, M_r indecomposable instead of strongly indecomposable.

2. If \mathcal{C} is the class of submodules of finite length, then $\mathcal{V}(\mathcal{C})$ is factorial.

Proof.

1. Follows from Theorem 2.44, Proposition 2.49 and Lemma 1.5.
2. Direct consequence of first point, thanks to Theorem 2.47.

□

We now proceed with

Proof of Proposition 2.49.

1. Let $M := M_1 \oplus M_2$ and suppose $M = N_1 \oplus \dots \oplus N_s$. For $i \in [1, r]$, let $\varepsilon_i : N_i \rightarrow M$ be the embedding and $p_i : M \rightarrow N_i$ the projection. Let $\alpha : M_1 \rightarrow M$ be the embedding and $\beta : M \rightarrow N_1$ the projection. Then

$$\beta \circ \alpha = \text{id}_{M_1} \quad \text{and} \quad \sum_{i=1}^s \varepsilon_i \circ p_i = \text{id}_M,$$

thus

$$\sum_{i=1}^s \beta \circ \varepsilon_i \circ p_i \circ \alpha = \text{id}_{M_1}.$$

Since $\text{End}_R(M_1)$ is local and id_{M_1} is invertible, there is at least one addendum $\beta \circ \varepsilon_i \circ p_i \circ \alpha$ which is invertible. Consider

$$\rho := p_i \circ \alpha \circ (\beta \circ \varepsilon_i \circ p_i \circ \alpha)^{-1} \circ \beta \circ \varepsilon_i \in \text{End}_R(N_i).$$

It is immediate to check that $\rho^2 = \rho$. Since N_i is indecomposable, by Exercise 27 this implies $\rho = 0$ or $\rho = \text{id}_{N_i}$. Since $\rho \circ p_i \circ \alpha = p_i \circ \alpha$ and $p_i \circ \alpha \neq 0$, it follows that $\rho \circ p_i \circ \alpha \neq 0$, and thus $\rho \neq 0$. Then $\rho = \text{id}_{N_i}$, and hence by definition of ρ we obtain that $p_i \circ \alpha : M_1 \rightarrow N_i$ is surjective.

Because $\beta \circ \varepsilon_i \circ p_i \circ \alpha$ is invertible, $p_i \circ \alpha$ is injective and thus $p_i \circ \alpha : M_1 \rightarrow N_i$ is an isomorphism. By Lemma 2.48 with

$$\varphi := \text{id}_M = \begin{pmatrix} p_i \circ \alpha & \bullet \\ \bullet & \bullet \end{pmatrix} : M_1 \oplus M_2 \rightarrow N_i \oplus \left(\sum_{\substack{j=1 \\ j \neq i}}^s N_j \right),$$

it follows that

$$M_2 \simeq \bigoplus_{\substack{j=1 \\ j \neq i}}^s N_j.$$

2. By induction on r . If $r = 1$ there is nothing to show. Let $r \geq 2$. If $M_1 \oplus \dots \oplus M_r \simeq N_1 \oplus \dots \oplus N_s$, then after renumbering if necessary we have $M_1 \simeq N_1$ and $M_2 \oplus \dots \oplus M_r \simeq N_2 \oplus \dots \oplus N_s$. By the induction hypothesis we are done.

□

2.5 Modules on Principal Ideal Domains

Definition 2.51. Let R be a domain and M an R -module.

1. $M_{\text{tor}} := \{x \in M \mid \text{Ann}_R(x) \neq 0\} \subseteq M$ is called *torsion module* of M . M is called

- *R -torsion free* if $M_{\text{tor}} = 0$.
- *R -torsion module* if $M_{\text{tor}} = M$.

2. For a prime element $p \in R$, let

$$M(p) := \{x \in M \mid \exists r \in \mathbb{N} \text{ such that } p^r x = 0\} \subseteq M$$

be the p -component of M . M is called *p -primary* if $M(p) = M$.

Theorem 2.52. Let R be a PID, P a set of representatives of prime elements in R , and M an R -torsion module. Then

$$M = \bigoplus_{p \in P} M(p).$$

If M is finitely generated, then $M(p) = 0$ for almost all $p \in P$.

Proof. Let $x \in M$, $\text{Ann}_R(x) = aR$ and $a = p_1^{k_1} \dots p_r^{k_r}$, where $r \in \mathbb{N}_0$, $p_1, \dots, p_r \in P$ and $k_1, \dots, k_r \in \mathbb{N}$. For $i \in [1, r]$, define $q_i := p_i^{-k_i} a \in R$. Then q_1, \dots, q_r are relatively prime and so there are $\alpha_1, \dots, \alpha_r \in R$ with $1 = q_1 \alpha_1 + \dots + q_r \alpha_r$. Then

$$x = q_1 \alpha_1 x + \dots + q_r \alpha_r x,$$

and for all $i \in [1, r]$ we have $p_i^{k_i} q_i \alpha_i x = a \alpha_i x = 0$, i.e. $q_i \alpha_i x \in M(p_i)$. Thus M is the sum of $(M(p))_{p \in P}$. It is left to show that the sum is direct. Take a $p \in P$ and let

$$x \in M(p) \cap \sum_{p' \in P \setminus \{p\}} M(p') = 0.$$

Let $p_1, \dots, p_n \in P \setminus \{p\}$ and $x = x_1 + \dots + x_n$ with $x_i \in M(p_i)$ for all $i \in [1, n]$. Let $r, r_1, \dots, r_n \in \mathbb{N}$ be such that

$$p^r x = p_1^{r_1} x_1 = \dots = p_n^{r_n} x_n = 0.$$

Since p^r and $p_1^{r_1} \cdot \dots \cdot p_n^{r_n}$ are relatively prime, there are $\alpha, \beta \in R$ such that $\alpha p^r + \beta p_1^{r_1} \cdot \dots \cdot p_n^{r_n} = 1$. Hence

$$x = \alpha p^r x + \beta p_1^{r_1} \cdot \dots \cdot p_n^{r_n} \underbrace{(x_1 + \dots + x_n)}_x = 0.$$

The last part of the statement is easy. \square

Remark. Recall that, by Theorem 2.25, R is a PID if and only if every submodule of a free module is free.

Theorem 2.53. Let R be a PID.

1. Let F be a f.g. free R -module and $M \subseteq F$ a submodule. Then there are an R -basis (u_1, \dots, u_n) of F , an $m \in [0, n]$, and $d_1, \dots, d_m \in R^\circ$ with $d_1 R \supseteq \dots \supseteq d_m R$ such that

$$(d_1 u_1, \dots, d_m u_m)$$

is an R -basis of M . Furthermore, the ideals $d_1 R, \dots, d_m R$ are uniquely determined.

2. Let M be a f.g. R -torsion module. Then there are $m \in \mathbb{N}_0$, $d_1, \dots, d_m \in R^\circ$ and $x_1, \dots, x_m \in M$ s.t.

(a) $M = Rx_1 \oplus \dots \oplus Rx_m$ and $\text{Ann}_R(x_i) = d_i R$ for all $i \in [1, m]$.

(b) $R \supsetneq d_1 R \supseteq d_2 R \supseteq \dots \supseteq d_m R$.

Furthermore, the ideals $d_1 R, \dots, d_m R$ are uniquely determined.

3. Let M be a f.g. R -module. Then there is a free module $K \subseteq M$ such that

$$M = M_{\text{tor}} \oplus K \quad \text{and} \quad K \simeq M/M_{\text{tor}}.$$

In particular, if M is torsionfree, then M is free.

The d_1, \dots, d_m are called the *elementary divisors* of M .

Proof.

Proof of existence in (1). We proceed by induction on $n = \text{rk}(F)$. If $n = 0$ or $M = 0$, then there is nothing to do. Suppose $M \neq 0$ and $n \geq 1$. We set $F^* := \text{Hom}_R(F, R)$. Consider

$$\{f[M] \triangleleft R \mid f \in F^*\}$$

and choose $f_1 \in F^*$ and $d_1 \in R$ such that $f_1[M] = d_1 R$ is maximal in the above set¹⁴. Furthermore, let $x_1 \in M$ be s.t. $f_1(x_1) = d_1$.

¹⁴Recall that a PID is a noetherian ring, since every ideal is trivially f.g.

Claim 1: $0 \neq x_1 \in d_1 F$.

Proof: Let (e_1, \dots, e_n) be a basis of F and (e_1^*, \dots, e_n^*) be the dual basis of F^* (i.e. $e_i^*(e_j) = \delta_{i,j}$, for all $i, j \in [1, n]$)¹⁵. If $0 \neq x \in M$, then there are $\lambda_1, \dots, \lambda_n \in R$ with $x = \lambda_1 e_1 + \dots + \lambda_n e_n$ and there is a $j \in [1, n]$ s.t. $\lambda_j \neq 0$. Then $0 \neq \lambda_j = e_j^*(x) \in e_j^*[M]$. This implies $d_1 R \neq 0$, and thus $x_1 \neq 0$.

It is left to show that $x_1 \in d_1 F$. We write

$$x_1 = \alpha_1 e_1 + \dots + \alpha_n e_n,$$

and for $\nu \in [1, n]$ we define

$$b_\nu R := \alpha_\nu R + d_1 R$$

and so we write $b_\nu = \alpha_\nu \beta_\nu + d_1 \rho_\nu$, for some $\beta_\nu, \rho_\nu \in R$.

Then, defining

$$g_\nu := \beta_\nu e_\nu^* + \rho_\nu f_1 \in F^*$$

we get $g_\nu(x_1) = \beta_\nu \alpha_\nu + \rho_\nu d_1 = b_\nu$, and hence

$$f_1[M] = d_1 R \subseteq b_\nu R \subseteq g_\nu[M].$$

Then the maximality of $f_1[M]$ implies $\alpha_\nu \in b_\nu R = d_1 R$ for all $\nu \in [1, n]$, and hence $x_1 = \sum_{\nu=1}^n \alpha_\nu e_\nu \in d_1 F$. ■

So we can write $x_1 = d_1 u_1$ for some $u_1 \in F$. Then $f_1(x_1) = d_1 = d_1 f_1(u_1)$ and hence $f_1(u_1) = 1$. We set

$$F_1 := \ker(f_1) \subseteq F \quad \text{and} \quad M_1 := M \cap F_1.$$

Claim 2: $F = Ru_1 \oplus F_1$ and $M = Rd_1 u_1 \oplus M_1$.

Proof: If $x \in F$, then $x - f_1(x)u_1 \in \ker(f_1) = F_1$,¹⁶ and hence $x = Ru_1 + \ker(f_1)$, i.e. $F = Ru_1 + F_1$.

If $x \in M$, then $f_1(x)u_1 \in d_1 Ru_1 = Rx_1 \subseteq M$, and hence $x - f_1(x)u_1 \in F_1 \cap M = M_1$, therefore $x \in Rd_1 u_1 + M_1$, i.e. $M = Rd_1 u_1 + M_1$.

Since $Rd_1 u_1 \cap M_1 \subseteq Ru_1 \cap F_1$, it is left to show only that $Ru_1 \cap F_1 = 0$. If $x \in Ru_1 \cap F_1$, then $x = \lambda u_1$ with $\lambda \in R$ and $0 = f_1(x) = \lambda \cdot 1 = \lambda$, which implies $x = 0$. ■

By Theorem 2.25, $F_1 \subseteq F$ is free and $\text{rk}(F_1) \leq \text{rk}(F)$. If $m \in \mathbb{N}$ and (v_2, \dots, v_m) is an R -basis of F_1 , then (u_1, v_2, \dots, v_m) is an R -basis of F by Claim 2. This implies that $m = n$ and F_1 is free of rank $n - 1$. By the induction hypothesis, there is an R -basis (u_2, \dots, u_n) of F_1 , $m \in [2, n]$ and $d_2, \dots, d_m \in R^\circ$ with $d_2 R \supseteq \dots \supseteq d_m R$ such that $(d_2 u_2, \dots, d_m u_m)$ is an R -basis of M_1 . Then (u_1, \dots, u_n) is an R -basis of F , $(d_1 u_1, d_2 u_2, \dots, d_m u_m)$ is an R -basis of M by Claim 2, and it is left to show

¹⁵Cfr. Exercise 34.

¹⁶ $f_1(x) - f_1(f_1(x)u_1) = f_1(x) - f_1(x)f_1(u_1) = f_1(x) - 1 \cdot f_1(x) = 0$.

$d_1R \supseteq d_2R$. Take $d \in R$ such that ${}_R\langle d_1, d_2 \rangle = dR$, and write $d = \alpha_1 d_1 + \alpha_2 d_2$ with $d_1, d_2 \in R$. Let (u_1^*, \dots, u_n^*) be the dual basis of F^* with respect to (u_1, \dots, u_n) . Then by defining

$$g := \alpha_1 u_1^* + \alpha_2 u_2^* \in F^* \text{ and } u := d_1 u_1 + d_2 u_2 \in M$$

we get $g(u) = d$, whence $d_1R \subseteq dR \subseteq g[M]$. The maximality of d_1R implies $d_1R = dR \supseteq d_2R$.

Proof of existence in (2) and (3). Let M be a f.g. R -module and F a f.g. free R -module of minimal rank such that there is an R -epimorphism $g : F \rightarrow M$.¹⁷ We set

$$M_1 := \ker g \quad \text{and} \quad g^* : F/M_1 \xrightarrow{\sim} M.$$

By (1), there is an R -basis (u_1, \dots, u_n) of F and an $m \in [0, n]$ and $d_1, \dots, d_m \in R^\circ$ with $d_1R \supseteq \dots \supseteq d_mR$ such that (d_1u_1, \dots, d_mu_m) is an R -basis of M_1 . For $i \in [1, m]$, we set $x_i := g(u_i)$. Then $M = {}_R\langle x_1, \dots, x_n \rangle$, and the minimality of the rank of F implies $x_i \neq 0$ for all $i \in [1, n]$. If

$$\begin{aligned} \varphi : R^n &\xrightarrow{\sim} F \\ (\lambda_1, \dots, \lambda_n) &\mapsto \sum_{i=1}^n \lambda_i u_i, \end{aligned}$$

then $M_1 = \varphi[d_1R \oplus \dots \oplus d_nR]$ (with $d_j = 0$ for all $j \in [m+1, n]$), and φ induces an R -isomorphism¹⁸

$$\varphi^* : R/d_1R \oplus \dots \oplus R/d_nR \rightarrow F/M_1.$$

Then we have

$$\begin{aligned} \Phi := g^* \circ \varphi^* : R/d_1R \oplus \dots \oplus R/d_nR &\rightarrow M \\ (\lambda_1 + d_1R, \dots, \lambda_n + d_nR) &\mapsto \lambda_1 x_1 + \dots + \lambda_n x_n. \end{aligned}$$

is an isomorphism. Thus $M = Rx_1 \oplus \dots \oplus Rx_n$, and $\text{Ann}_R(x_i) = \text{Ann}_R(\Phi^{-1}(x_i)) = \text{Ann}_R(1 + d_iR) = d_iR$ for all $i \in [1, n]$.

Since $x_1 \neq 0$, we get $d_1R = \text{Ann}_R(x_1) \subsetneq R$.

Finally, observe that $M_{\text{tor}} = Rx_1 \oplus \dots \oplus Rx_m$ and $K = Rx_{m+1} \oplus \dots \oplus Rx_n$ is R -free with basis (x_{m+1}, \dots, x_n) (to see this, look back at how g^* works).

Proof of uniqueness in (2) and (3). We proceed by induction on m . If $m = 1$, ok. Suppose $m \geq 2$. If

$$N = R/d_1R \oplus \dots \oplus R/d_mR \simeq R/d'_1R \oplus \dots \oplus R/d'_mR$$

¹⁷Such a module exists thanks to Theorem 2.27.

¹⁸Here we are using the fact that if $\varphi : A \rightarrow A'$ is an isomorphism and $B \subseteq A$, then $A/B \simeq A'/\varphi[B]$. Furthermore, it is easy to check that $R^n/d_1R \oplus \dots \oplus d_nR \simeq R/d_1R \oplus \dots \oplus R/d_nR$.

with $m, m' \in \mathbb{N}$, $R \supsetneq d_1 R \supseteq \dots \supseteq d_m R$ and $R \supsetneq d'_1 R \supseteq \dots \supseteq d'_{m'} R$, then

$$d_m R = \text{Ann}_R(R/d_1 R \oplus \dots \oplus R/d_m R) = \text{Ann}_R(R/d'_1 R \oplus \dots \oplus R/d'_{m'} R) = d'_{m'} R.$$

Since

$$\begin{aligned} R/d_1 R \oplus \dots \oplus R/d_{m-1} R &\simeq (R/d_1 R \oplus \dots \oplus R/d_m R)/(0, \dots, 0, R/d_m R) \\ &\simeq (R/d'_1 R \oplus \dots \oplus R/d'_{m'} R)/(0, \dots, 0, R/d'_{m'} R) \simeq R/d'_1 R \oplus \dots \oplus R/d'_{m'-1} R, \end{aligned}$$

the assertion follows from the inductive hypothesis.

Proof of uniqueness in (1). If M and d_1, \dots, d_m are as in (1), then following the proof of (2) we can find x_1, \dots, x_m such that

$$(F/M)_{\text{tor}} = Rx_1 \oplus \dots \oplus Rx_m.$$

Then the assertion follows from the uniqueness in (2). \square

Remark 2.54 (Linear equations systems over PIDs). Let R be a PID, $m, n \in \mathbb{N}$, $b \in R^m$, $A \in \mathcal{M}_{m,n}(R)$ and

$$\begin{aligned} \theta_A: R^n &\rightarrow R^m \\ \mathbf{x} &\mapsto A\mathbf{x}. \end{aligned}$$

We set

$$L_k^R(A) := L_k(A) := \ker \theta_A = \{\mathbf{x} \in R^n \mid A\mathbf{x} = 0\}$$

and

$$L(A, b) := \{\mathbf{x} \in R^n \mid A\mathbf{x} = b\}.$$

1. $L_k(A) \subseteq R^n$ is an R -submodule and for all $x_0 \in L(A, b)$ we have $L(A, b) = x_0 + L_k(A)$. If $A = (a_1, \dots, a_n)$ with $a_1, \dots, a_n \in \mathcal{M}_{m,1}(R)$, then

$$L(A, b) \neq \emptyset \Leftrightarrow b \in {}_R\langle a_1, \dots, a_n \rangle \subseteq R^m.$$

2. Two matrices $A, B \in \mathcal{M}_{m,n}(R)$ are called equivalent (and we write $A \sim B$) if there are matrices $U \in \text{GL}_m(R)$ and $V \in \text{GL}_n(R)$ such that $B = UAV$. For $\mathbf{x} \in R^n$ we have

$$B\mathbf{x} = 0 \Leftrightarrow U^{-1}B\mathbf{x} = 0 \Leftrightarrow AV\mathbf{x} = 0 \Leftrightarrow A\mathbf{x} = 0.$$

3. (Smith Normal Form). There are uniquely determined $r \in [1, \min(m, n)]$ and $d_1, \dots, d_r \in R^\circ$ such that $d_1 R \supseteq \dots \supseteq d_r R$ and

$$A \sim \begin{pmatrix} d_1 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & d_2 & \dots & \dots & \dots & \dots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots & \vdots & 0 \\ \vdots & \vdots & \dots & d_r & 0 & \dots & 0 \\ \vdots & \vdots & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} =: D.$$

Proof. Let $\mathbf{e}^n := (e_1, \dots, e_n)$ and $\mathbf{e}^m := (e_1, \dots, e_m)$ be homogeneous bases of R^n and R^m respectively. Then

$$(\theta_A(e_1), \dots, \theta_A(e_n)) = (e_1, \dots, e_n) \mathcal{M}_{\mathbf{e}^n, \mathbf{e}^m}(\theta_A) = (e_1, \dots, e_n) A.$$

D is called *Smith Normal Form* of A .

Uniqueness. If $A \sim D$, then there are R -bases \mathbf{u} of R^n and \mathbf{v} of R^m with $\mathcal{M}_{\mathbf{u}, \mathbf{v}}(\theta_A) = D$, and $(d_1 v_1, \dots, d_r v_r)$ is an R -basis of $\text{Im}(\theta_A)$. By Theorem 2.53, the $d_1 R, \dots, d_r R$ are uniquely determined.

Existence. By Theorem 2.25, $0 \neq \text{Im}(\theta_A) \subseteq R^m$ is a free submodule with rank $r \in [1, n]$. By Theorem 2.53, there is a basis (v_1, \dots, v_m) of R^m and $d_1, \dots, d_r \in R^\circ$ with $d_1 R \supseteq \dots \supseteq d_r R$ such that $(d_1 v_1, \dots, d_r v_r)$ is an R -basis of $\text{Im}(\theta_A)$. There is an R -monomorphism ψ such that

$$0 \longrightarrow \ker(\theta_A) \hookrightarrow R^n \xrightarrow{\theta_A} \text{Im}(\theta_A) \longrightarrow 0$$

$\swarrow \text{---} \psi \text{---}$

with $\theta_A \circ \psi = \text{id}_{\text{Im}(\theta_A)}$ and $R^n = \text{Im}(\psi) \oplus \ker(\theta_A)$ (cfr. Exercise 33). Then

$$\ker(\theta_A|_{\text{Im}(\psi)}) = \ker(\theta_A) \cap \text{Im}(\psi) = 0 \quad \text{and} \quad \text{Im}(\theta_A) = \theta_A[\text{Im}(\psi)].$$

Thus $\theta_A|_{\text{Im}(\psi)} : \text{Im}(\psi) \xrightarrow{\sim} \text{Im}(\theta_A)$.

So there exists an R -basis \mathbf{u}' of $\text{Im}(\psi)$ such that $\theta_A(\mathbf{u}') = (d_1 v_1, \dots, d_r v_r)$. By Theorem 2.25, $\ker(\theta_A) \subseteq R^n$ is free and thus there exists an R -basis \mathbf{u}'' of $\ker(\theta_A)$. Then $\mathbf{u} := (\mathbf{u}', \mathbf{u}'')$ is an R -basis of R^n with

$$\theta_A(\mathbf{u}) = (\theta_A(\mathbf{u}'), 0) = \underbrace{(v_1, \dots, v_m)}_{1 \times m} \underbrace{D}_{m \times n}$$

with D as in the claim, i.e. $D = \mathcal{M}_{\mathbf{u}, \mathbf{v}}(\theta_A) \sim A$. □

Chapter 3

Ideal Theory

Throughout this whole chapter, R is a ring.

3.1 Prime ideals and maximal ideals

3.1. Krull's Existence Theorem. Let $I \triangleleft R$ be an ideal, $T \subseteq R$ a multiplicatively closed subset of R with $T \cap I = \emptyset$ and let $\Omega = \{J \triangleleft R \mid I \subseteq J, J \cap T = \emptyset\}$. Then:

1. Ω has a maximal element w.r.t. set-inclusion.
2. Every maximal element of Ω is a prime ideal. Particularly, there is a prime ideal P with $I \subseteq P$ and $T \cap P = \emptyset$.

Proof.

1. If $\Sigma \subseteq \Omega$ is a chain, the $\bigcup_{Q \in \Sigma} Q$ is an upper bound for Σ . Thus the preconditions of Zorn's lemma are satisfied and Ω has a maximal element.
2. Let $P \in \Omega$ be maximal and let $a, b \in R$ with $ab \in P$. Suppose towards a contradiction that $a \notin P$ and $b \notin P$. Then $P + aR \notin \Omega$ and $P + bR \notin \Omega$. By definition of Ω , this means $(P + aR) \cap T \neq \emptyset$ and $(P + bR) \cap T \neq \emptyset$. Let then $p_1, p_2 \in P$ and $c_1, c_2 \in R$ be such that $p_1 + c_1a \in T$ and $p_2 + c_2b \in T$. Then

$$(p_1 + c_1a)(p_2 + c_2b) = (p_2 + c_2b)p_1 + (c_1a)p_2 + (c_1c_2)ab \in P \cap T = \emptyset,$$

contradiction.

□

Corollary 3.2. Let $R \neq 0$.

1. Every proper ideal $I \triangleleft R$ is contained by a maximal ideal. In particular, $\max(R) \neq \emptyset$.
2. For all $a \in R \setminus R^\times$ there is a $m \in \max(R)$ with $a \in m$.

Proof.

1. We use last theorem with $T = \{1\}$. Since $J = 0 \subsetneq R$, we get $\max(R) \neq \emptyset$.
2. Follows from (1) with $I = aR$.

□

3.3. Cohen's Theorem. If every prime ideal of R is finitely generated, then R is noetherian.

Proof. We proceed by contraposition: suppose R is not noetherian. We shall find a prime ideal which is not finitely generated.

Let $\Omega := \{J \triangleleft R \mid J \text{ not finitely generated}\} \neq \emptyset$.

Claim 1: Chains in Ω have upper bounds.

Proof: Let $\Sigma \subseteq \Omega$ be a chain and let $I = \bigcup_{Q \in \Sigma} Q$. Then $I \subseteq R$ is an ideal. Suppose I is finitely generated, i.e. $I = \langle a_1, \dots, a_n \rangle$. Then there exists $Q \in \Sigma$ such that $a_1, \dots, a_n \in Q$, which means $I \subseteq Q \subseteq I$, that is $I = Q$. Thus Q is finitely generated, contradiction. ■

Therefore, by Zorn's lemma, Ω has a maximal element P . Of course, since $P \in \Omega$, P is not finitely generated. If we show that P is prime, we are done.

Claim 2: P is a prime ideal.

Proof: Suppose to the contrary that there exist $a, b \in R \setminus P$ s.t. $ab \in P$. Since $P \subsetneq P + aR$, then $P + aR \notin \Omega$, i.e. $P + aR$ is finitely generated. Let $P + aR = \langle p_1 + c_1a, \dots, p_k + c_ka \rangle$ with $p_i \in P$, $c_i \in R$. Consider $J := \{y \in R \mid ya \in P\} \subseteq R$, which is an ideal¹. We have $P \subsetneq P + Ra \subseteq J$, where the last inclusion follows immediately by $ab \in P$. Therefore J is finitely generated as well, i.e. $J = \langle b_1, \dots, b_l \rangle$ for some $b_1, \dots, b_l \in R$. We now want to show that $P = \langle p_1, \dots, p_k, b_1a, \dots, b_la \rangle$, which contradicts the fact that P is not finitely generated. The inclusion " \supseteq " is trivial. In order to prove " \subseteq ", let $x \in P$. Since $P \subseteq P + aR$, we have

$$x = \sum_{i=1}^k \lambda_i(p_i + c_ia) \quad \text{for some } \lambda_1, \dots, \lambda_k \in R.$$

¹More in general, we define the *ideal quotient* of two ideals I, I' as $(I : I') := \{x \in R \mid xI' \subseteq I\}$. So, in our case, $J = (P : Ra)$.

Then $\left(\sum_{i=1}^k \lambda_i c_i\right)a = x - \sum_{i=1}^k \lambda_i p_i \in P$. This means $\sum_{i=1}^k \lambda_i c_i \in J$, thus $\sum_{i=1}^k \lambda_i c_i = \sum_{j=1}^l \mu_j b_j$ with $\mu_1, \dots, \mu_l \in R$. Finally we get

$$x = \sum_{i=1}^k \lambda_i p_i + a \sum_{j=1}^l \mu_j b_j \in \langle p_1, \dots, p_k, b_1 a, \dots, b_l a \rangle.$$

■

So P is a prime ideal, and it's not finitely generated, as wanted. \square

Addendum. For commutative rings, an ideal P is prime if and only if $P \neq R$ and for all ideals A, B of R , if $AB \subseteq P$ then $A \subseteq P$ or $B \subseteq P$. (see <http://math.stackexchange.com/questions/73213/equivalence-of-definitions-of-prime-ideal-in-commutative-ring>)

Theorem 3.4. Let $k \geq 2$.

1. If $P \in \text{Spec}(R)$, $I_1, \dots, I_k \triangleleft R$ and $\bigcap_{j=1}^k I_j \subseteq P$, then $I_j \subseteq P$ for some $j \in [1, k]$.
2. If $P_1, \dots, P_k \in \text{Spec}(R)$, $I \triangleleft R$ and $I \subseteq \bigcup_{j=1}^k P_j$, then $I \subseteq P_j$ for some $j \in [1, k]$.

Proof.

1. Remember that $I_1 \cdot \dots \cdot I_k \subseteq I_1 \cap \dots \cap I_k$, thus $I_1 \cdot \dots \cdot I_k \subseteq P$, and thus $I_j \subseteq P$ for some j , since P is prime.
2. We proceed by induction on k . Let $k = 2$. Assume to the contrary that $I \not\subseteq P_1$ and $I \not\subseteq P_2$. Let $a_j \in I \setminus P_j$, with $j = 1, 2$. Since $I \subseteq P_1 \cup P_2$, we have $a_2 \in P_1$. Furthermore, $a_1 + a_2 \in I \subseteq P_1 \cup P_2$. Suppose w.l.o.g. $a_1 + a_2 \in P_1$. But then $a_1 = (a_1 + a_2) - a_2 \in P_1$, contradiction. Suppose now that $k \geq 3$ and that the assertion holds for $k - 1$. If there exists a $\bar{j} \in [1, k]$ with

$$I \subseteq \bigcup_{\substack{j=1 \\ j \neq \bar{j}}}^k P_j,$$

then the statement follows by the induction hypothesis. So we may assume w.l.o.g. (towards a contradiction) that for all $j \in \{1, \dots, k\}$ there exists

$$a_j \in I \setminus \bigcup_{\substack{i=1 \\ i \neq j}}^k P_i \subseteq P_j.$$

Consider then $a = a_1 \cdot \dots \cdot a_{k-1} + a_k \in I$. If $a \in P_j$ for some $j \in [1, k - 1]$, then $a_k = a - a_1 \cdot \dots \cdot a_{k-1} \in P_j$, contradiction. So necessarily $a \in P_k$, thus $a - a_k = a_1 \cdot \dots \cdot a_{k-1} \in P_k$, and since P_k is prime this means $a_j \in P_k$ for some $j \in [1, k]$, again a contradiction.

□

Lemma 3.5. Let $f : R \rightarrow S$ be a ring homomorphism.

1. If $Q \triangleleft S$ is prime, then $f^{-1}[Q] \triangleleft R$ is prime.
2. If f is surjective and $Q \triangleleft S$ is maximal, then $f^{-1}[Q]$ is maximal.

Lemma 3.6. The following statements are equivalent:

1. $|\max(R)| = 1$.
2. $R \setminus R^\times \subseteq R$ is an ideal.

Definition 3.7. A ring R is called

- *local* if $R \setminus R^\times$ is an ideal (see 2.46!).
- *semilocal* if $|\max(R)| < \infty$.

Remark.

1. Every field is local.
2. If $p \in \mathbb{P}$, then

$$\mathbb{Z}_{(p)} = \left\{ x \in \mathbb{Q} \mid x = \frac{a}{s}, a \in \mathbb{Z}, s \in \mathbb{N} \setminus p\mathbb{N} \right\} \subseteq \mathbb{Q}$$

is a local ring (since $R \setminus R^\times = pR$).

Definition 3.8. Ideals $(Q_i)_{i \in I}$ of R are called (pairwise) comaximal if $Q_i + Q_j = R$ for all $i \neq j \in I$.

Theorem 3.9. Let $m \geq 2$, $(Q_j)_{j=1}^m$ be a family of comaximal ideals with $Q_j \neq R$ for all $j \in [1, m]$. The following holds:

1. $Q_1 \cap \dots \cap Q_{m-1}$ and Q_m are comaximal.
2. $Q_1 \cap \dots \cap Q_m = Q_1 \cdot \dots \cdot Q_m$.
3. (Chinese Remainder Theorem) The map

$$\begin{aligned} \varphi : R &\rightarrow \prod_{i=1}^m R/Q_i \\ a &\mapsto (a + Q_1, \dots, a + Q_m) \end{aligned}$$

is a ring epimorphism with $\ker \varphi = \prod_{i=1}^m Q_i$.

Proof.

1. Suppose $m \geq 3$ and define $Q = Q_1 \cap \dots \cap Q_{m-1}$. Assume to the contrary that Q and Q_m are not comaximal. Then there is a maximal ideal \mathfrak{m} with $Q + Q_m \subseteq \mathfrak{m}$. Then $Q \subseteq \mathfrak{m}$, and thus by 3.4.(1) $Q_j \subseteq \mathfrak{m}$ for some $j \in [1, m-1]$. This implies $Q_j + Q_m \subseteq \mathfrak{m}$, but this is impossible, since $Q_j + Q_m = R$.
2. It suffices to show " \subseteq ". We proceed by induction on m . If $m = 2$, then

$$\begin{aligned} Q_1 \cap Q_2 &= (Q_1 \cap Q_2)R = (Q_1 \cap Q_2)(Q_1 + Q_2) \\ &= \underbrace{(Q_1 \cap Q_2)Q_1}_{\subseteq Q_2} + \underbrace{(Q_1 \cap Q_2)Q_2}_{\subseteq Q_1} \subseteq Q_1 Q_2. \end{aligned}$$

Let $m \geq 3$. By induction hypothesis we have $Q := \bigcap_{j=1}^{m-1} Q_j = \prod_{j=1}^{m-1} Q_j$. Thanks to point (1), Q and Q_m are comaximal, and thus, again by induction hypothesis we obtain

$$\bigcap_{j=1}^m Q_j = Q \cap Q_m = Q \cdot Q_m = \prod_{j=1}^m Q_j.$$

3. Obviously, φ is a ring homomorphism with $\ker \varphi = \bigcap_{i=1}^m Q_i = \prod_{i=1}^m Q_i$. In order to show that φ is surjective, let $x_1, \dots, x_m \in R$. For all $j \in [1, m]$, the ideals Q_j and $\prod_{i \neq j}^m Q_i$ are comaximal (by (1) and (2)), and hence there exist $u_j \in Q_j$ and $v_j \in \prod_{i \neq j}^m Q_i$ such that $u_j + v_j = 1$. Therefore $v_j \equiv \delta_{ij} \pmod{Q_i}$, for $i \in [1, m]$, and hence

$$x := \sum_{k=1}^m v_k x_k \equiv x_i \pmod{Q_i}$$

for all $j \in [1, m]$. This means that x is a preimage for $(x_1 + Q_1, \dots, x_m + Q_m)$. □

3.2 Nakayama's Lemma and Krull's Intersection Theorem

Definition 3.10. Given an R -module M , the *Jacobson radical* of M is

$$\mathcal{J}(M) := \bigcap_{\substack{N \subseteq M \\ N \text{ maximal}}} N.$$

If there are no maximal submodules, then $\mathcal{J}(M) := M$.

If $M = R$, then $\mathcal{J}(R)$ is the Jacobson radical of R .

Remarks and Examples.

1. $\mathcal{J}(M)$ is trivially a submodule of M .
2. If M is simple, then $\mathcal{J}(M) = \{0\}$.
3. $\mathcal{J}(M) = \bigcap_{\substack{\varphi: M \rightarrow E \\ E \text{ simple}}} \ker(\varphi).$

Proof. If $\varphi \neq 0$, then φ is surjective, so $M/\ker(\varphi) \simeq E$, and hence $\ker(\varphi) \subseteq M$ is maximal (this is immediate to see using 2.9).

Conversely, every maximal submodule $N \subseteq M$ is the kernel of the canonical epimorphism $M \rightarrow M/N$, and M/N is simple. \square

4. $\mathcal{J}(\mathbb{Z}) = \bigcap_{p \in \mathbb{P}} p\mathbb{Z} = \{0\}.$
5. $\mathcal{J}(R) = \{x \in R \mid 1 + Rx \subseteq R^\times\}.$

Proof.

“ \subseteq ” Let $x \in \mathcal{J}(R)$ and $a \in R$. Assume to the contrary that $1 + ax \notin R^\times$. By Corollary 3.2, there is an $\mathfrak{m} \in \max(R)$ such that $1 + ax \in \mathfrak{m}$. Since $ax \in \mathcal{J}(R)$, then $ax \in \mathfrak{m}$, and it follows that $1 \in \mathfrak{m}$, contradiction.

“ \supseteq ” Let $x \in R$ such that $1 + Rx \subseteq R^\times$. Assume to the contrary that there is an $\mathfrak{m} \in \max(R)$ such that $x \notin \mathfrak{m}$. Then $R = \mathfrak{m} + Rx$, whence $1 = m + ax$ for some $m \in \mathfrak{m}$, $a \in R$, and thus $m = 1 - ax \in 1 + Rx \subseteq R^\times$, contradiction. \square

Lemma 3.11.

1. If $\varphi : M_1 \rightarrow M_2$ is an R -homomorphism, then $\varphi[\mathcal{J}(M_1)] \subseteq \mathcal{J}(M_2).$
2. If $N \subseteq M$ is a submodule with $N \subseteq \mathcal{J}(M)$, then $\mathcal{J}(M/N) = \mathcal{J}(M)/N.$
3. $\mathcal{J}(M/\mathcal{J}(M)) = 0.$

Proof.

1. If E is simple and $\psi : M_2 \rightarrow E$ is a homomorphism, then $\psi \circ \varphi : M_1 \rightarrow E$ is a homomorphism, and hence $\mathcal{J}(M_1) \subseteq \ker(\psi \circ \varphi)$. Then $\varphi[\mathcal{J}(M_1)] \subseteq \ker(\psi)$. Since $\mathcal{J}(M_2)$ is the intersection of all such $\ker(\psi)$'s, by the arbitrariness of ψ and E it follows that $\varphi[\mathcal{J}(M_1)] \subseteq \mathcal{J}(M_2).$

2. The maximal submodules of M/N are precisely the ones of the form M'/N with $M' \subseteq M$ maximal and $N \subseteq M'$. Since $N \subseteq \mathcal{J}(M)$, we always have $N \subseteq M'$. Thus

$$\mathcal{J}(M/N) = \bigcap_{\substack{M' \subseteq M \\ M' \text{ maximal}}} (M'/N) = \left(\bigcap_{\substack{M' \subseteq M \\ M' \text{ maximal}}} M' \right) / N = \mathcal{J}(M)/N.$$

3. Follows from (2) with $N = \mathcal{J}(M)$.

□

Definition 3.12. A submodule $M' \subseteq M$ is called *superfluous in M* if the following condition holds:

$$N + M' = M \implies N = M, \quad \text{for all } N \subseteq M.$$

Proposition 3.13.

1. The following statements are equivalent:
 - a) M is finitely generated.
 - b) $M/\mathcal{J}(M)$ is finitely generated and $\mathcal{J}(M)$ is superfluous.
2. $\mathcal{J}(R)M \subseteq \mathcal{J}(M)$.
3. **Nakayama's Lemma:**

If M is finitely generated, then $\mathcal{J}(R)M$ is superfluous.

Proof.

1. “(a) \implies (b)” Since factor modules of finitely generated modules are finitely generated (see 2.34), $M/\mathcal{J}(M)$ is finitely generated. Let $N \subsetneq M$ be a submodule. By Exercise 35, there is a maximal submodule $N \subseteq M' \subsetneq M$. This implies $\mathcal{J}(M) \subseteq M'$, $N + \mathcal{J}(M) \subseteq M'$ and hence $N + \mathcal{J}(M) \neq M$.

“(b) \implies (a)” Let $x_1, \dots, x_n \in M$ be such that

$$M/\mathcal{J}(M) = \sum_{i=1}^n R(x_i + \mathcal{J}(M)).$$

Then $M = (\sum_{i=1}^n Rx_i) + \mathcal{J}(M)$, and since $\mathcal{J}(M)$ is superfluous we get $M = \sum_{i=1}^n Rx_i$.

2. For all $x \in M$, the map $R \rightarrow M$ given by $\lambda \mapsto \lambda x$ is an R -homomorphism. Thus Lemma 3.11(1) implies that $\mathcal{J}(R)x \subseteq \mathcal{J}(M)$, and hence $\mathcal{J}(R)M \subseteq \mathcal{J}(M)$.
3. Since M is finitely generated, point (1) implies that $\mathcal{J}(M)$ is superfluous, and by point (2) it follows that $\mathcal{J}(R)M \subseteq \mathcal{J}(M)$ is superfluous.

□

Corollary 3.14. Let M be an R -module and $I \subseteq \mathcal{J}(R)$ an ideal. The following statements hold:

1. If M is finitely generated and $IM = M$, then $M = 0$.
2. If $N \subseteq M$ is a submodule such that M/N is finitely generated and $M = N + IM$, then $M = N$.

Proof. Exercise. □

3.15. Krull's intersection theorem. Let R be a noetherian ring, M a finitely generated R -module, and $I \triangleleft R$. The following statements hold:

1. If $N = \bigcap_{n \geq 0} I^n M$, then $IN = N$.
2. If $I \subseteq \mathcal{J}(R)$, then $\bigcap_{n \geq 0} I^n M \stackrel{(i)}{=} 0$ and $\bigcap_{n \geq 0} I^n \stackrel{(ii)}{=} 0$.
3. If $N \subseteq M$ and $I \subseteq \mathcal{J}(R)$, then $N = \bigcap_{n \geq 0} (N + I^n M)$.

Proof.

1. Let $N = \bigcap_{n \geq 0} I^n M$, and $\Omega = \{L \subseteq M \mid IN \subseteq L, IN = L \cap N\}$. From $IN \in \Omega$ follows $\Omega \neq \emptyset$. By Corollary 2.36, M is noetherian, and thus Ω has a maximal element L .

Claim: There is an $h \in \mathbb{N}$ with $I^h M \subseteq L$.

Proof: We will show that for every $c \in I$ there is an $n \in \mathbb{N}$ such that $c^n M \subseteq L$. Then, since R is noetherian, there are $a_1, \dots, a_k \in I$ such that $I = \langle a_1, \dots, a_k \rangle$. So there is an $n' \in \mathbb{N}$ with $a_i^{n'} M \subseteq L$ for all $i \in [1, k]$. Define $h := n'k$. By Exercise 40 we have

$$I^h M \subseteq \langle a_1^h, \dots, a_k^h \rangle M = \sum_{i=1}^k a_i^h M \subseteq L.$$

Let $c \in I$. If $m \in \mathbb{N}$ and $M_m = \{x \in M \mid c^m x \subseteq L\}$, then $M_1 \subseteq M_2 \subseteq \dots$ is an ascending chain², and thus there is an $n \in \mathbb{N}$ such that $M_m = M_n$ for all $m \geq n$. We claim that

$$(c^n M + L) \cap N = IN. \quad (*)$$

Then $c^n M + L \in \Omega$, thus $c^n M + L = L$ by maximality of L , and hence $c^n M \subseteq L$, as wanted.

Let's show (*). The inclusion " \supseteq " is trivial, since $IN \subseteq N$ and $IN \subseteq L$. As for " \subseteq ", let $z = c^n x + y \in (c^n M + L) \cap N$ with $x \in M$ and $y \in L$. Then $cz = c^{n+1}x + cy \in cN \subseteq L$, and thus $c^{n+1}x = cz - cy \in L$, i.e. $x \in M_{n+1} = M_n$. Thus $c^n x \in L$ and therefore $z \in L \cap N = IN$. \blacksquare

So we have $N \subseteq I^h M \subseteq L$, and thus $N \subseteq I^h M \cap N \subseteq L \cap N = IN \subseteq N$, i.e. $N = IN$.

2. Let $N = \bigcap_{n \geq 0} I^n M$. By the first point, we have $IN = N$, thus $N = 0$ by Corollary 3.14(1). Thus equality (i) follows. Equality (ii) follows from (i) with $M = R$.
3. By the second point, we have $\bigcap_{n \geq 0} I^n(M/N) = 0$. Consider $\pi : M \rightarrow M/N$. Then

$$\begin{aligned} N = \pi^{-1}(0) &= \pi^{-1}\left(\bigcap_{n \geq 0} I^n(M/N)\right) = \bigcap_{n \geq 0} \pi^{-1}\left(I^n(M/N)\right) \\ &\stackrel{3}{=} \bigcap_{n \geq 0} \pi^{-1}\left((I^n M + N)/N\right) = \bigcap_{n \geq 0} (I^n M + N). \end{aligned}$$

\square

Definition 3.16. Let R be a ring and $I \triangleleft R$. Then the *variety* of I is

$$\mathcal{V}(I) = \{\mathfrak{p} \in \text{Spec}(R) \mid I \subseteq \mathfrak{p}\}.$$

The minimal elements of $\mathcal{V}(I)$ are called *prime divisors of I* , and $\mathbb{P}(I)$ is the set of minimal prime divisors of I . The set $\mathbb{P}(0)$ contains exactly the minimal prime ideals of R .

If $\mathfrak{p} \in \text{Spec}(R)$, then $\mathbb{P}(\mathfrak{p}) = \{\mathfrak{p}\}$.

Lemma 3.17. If $\Sigma \subseteq \text{Spec}(R)$ is a chain, then $\bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$ and $\bigcap_{\mathfrak{p} \in \Sigma} \mathfrak{p}$ are prime ideals.

²if $c^m x \in L$, then also $c^{m+1}x \in L$, since L is a module.

³Observe that $[\lambda x + y] = [\lambda x] = \lambda[x]$.

Theorem 3.18. Let $I \triangleleft R$. Then

1. For all $\mathfrak{p} \in \mathcal{V}(I)$ there is a $\mathfrak{p}_0 \in \mathbb{P}(I)$ such that $\mathfrak{p}_0 \subseteq \mathfrak{p}$.
2. If R/I is noetherian, then there are $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \mathbb{P}(I)$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq I$.
Particularly, every noetherian domain has only finitely many prime ideals.

Proof.

1. Let $\mathfrak{p} \in \mathcal{V}(I)$. Define $\Omega := \{\mathfrak{p}' \in \mathcal{V}(I) \mid \mathfrak{p}' \subseteq \mathfrak{p}\}$. We define the partial order \leq on Ω given by reverse inclusion, i.e. $\mathfrak{p}' \leq \mathfrak{p}'' \Leftrightarrow \mathfrak{p}' \supseteq \mathfrak{p}''$.
If $\Sigma \subseteq \Omega$ is a chain, then by Lemma 3.17 it follows that $\bigcap_{\mathfrak{q} \in \Sigma} \mathfrak{q} \in \Omega$. Then Ω has a maximal element \mathfrak{p}_0 by Zorn's Lemma.
2. Let $X := \{\mathfrak{p}_1 \dots \mathfrak{p}_n \mid n \in \mathbb{N}, \mathfrak{p}_1, \dots, \mathfrak{p}_n \in \mathbb{P}(I)\}$. Suppose towards a contradiction that for all $\mathfrak{a} \in X$ it holds $\mathfrak{a} \not\subseteq I$. Then

$$I \in \Sigma := \left\{ J \triangleleft R \mid I \subseteq J, \forall \mathfrak{a} \in X [\mathfrak{a} \not\subseteq J] \right\}.$$

Since R/I is noetherian, Σ has a maximal element \mathfrak{q} .

Claim: $\mathfrak{q} \in \text{Spec}(R)$.

Proof: Suppose there are $a, b \in R \setminus \mathfrak{q}$ with $ab \in \mathfrak{q}$. Then $\mathfrak{q} + aR \not\subseteq \Sigma$ and $\mathfrak{q} + bR \not\subseteq \Sigma$. Hence there are $\mathfrak{a}_1, \mathfrak{a}_2 \in X$ such that $\mathfrak{a}_1 \subseteq \mathfrak{q} + aR$ and $\mathfrak{a}_2 \subseteq \mathfrak{q} + bR$ and thus

$$\mathfrak{a}_1 \mathfrak{a}_2 \subseteq (\mathfrak{q} + aR)(\mathfrak{q} + bR) \subseteq \mathfrak{q},$$

which contradicts $\mathfrak{q} \in \Sigma$, since obviously $\mathfrak{a}_1 \mathfrak{a}_2 \in X$. ■

By point (1), there is a $\mathfrak{p}_0 \in \mathbb{P}(I)$ with $\mathfrak{p}_0 \subseteq \mathfrak{q}$. But obviously $\mathfrak{p}_0 \in X$, and this contradicts $\mathfrak{q} \in \Sigma$. The proof is complete.

In order to show that every noetherian domain has only finitely many prime ideals, consider $\{0\} \triangleleft R$, which is prime since R is a domain. Of course $R/\{0\}$ is noetherian and $\mathbb{P}(\{0\})$ are the minimal prime ideals of R . Thus, there exist $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \mathbb{P}(\{0\})$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq \{0\}$. Now take a prime ideal \mathfrak{p} . Of course, $\{0\} \subseteq \mathfrak{p}$, and hence $\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq \mathfrak{p}$. Since \mathfrak{p} is prime, we have $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some $i \in [1, n]$. (??? sì ma a me serve $\mathfrak{p} = \mathfrak{p}_i$!)

□

3.3 Hilbert's Basis Theorem.

3.19. Hilbert's Basis Theorem. Let R be noetherian and $n \in \mathbb{N}$. Then $R[X_1, \dots, X_n]$ is noetherian.

Proof. If we show the statement for $n = 1$, the general statement follows immediately by induction, since $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$. Suppose there is an $I \triangleleft R[X]$ which is not finitely generated. Let $0 \neq f_1 \in I$ of minimal degree. For $k \geq 1$, we recursively define a sequence $(f_k)_{k \geq 1}$ such that

$$0 \neq f_{k+1} \in I \setminus \langle f_1, \dots, f_k \rangle$$

and f_{k+1} is of minimal degree. For $k \in \mathbb{N}$, let $n_k = \deg(f_k)$ and $a_k \in R$ be the leading coefficient of f_k . Then $n_1 \leq n_2 \leq \dots$ and ${}_R\langle a_1 \rangle \subseteq {}_R\langle a_1, a_2 \rangle \subseteq \dots$ is an ascending chain of ideals.

Since R is noetherian, there exists $k \in \mathbb{N}$ such that ${}_R\langle a_1, \dots, a_{k'} \rangle = {}_R\langle a_1, \dots, a_k \rangle$ for every $k' \geq k$. Then there are $b_1, \dots, b_k \in R$ with $a_{k+1} = \sum_{i=1}^k b_i a_i$ and we have

$$g := f_{k+1} - \sum_{i=1}^k b_i X^{n_{k+1}-n_i} f_i \in I \setminus \langle f_1, \dots, f_k \rangle$$

with $\deg(g) < \deg(f_{k+1})$, contradiction.

Observe that $g \notin \langle f_1, \dots, f_k \rangle$ because otherwise $f_{k+1} = g + \sum_{i=1}^k b_i X^{n_{k+1}-n_i} f_i \in \langle f_1, \dots, f_k \rangle$. \square

Corollary 3.20. Let $R \subseteq S$ be commutative rings, with S finitely generated on R as a ring (i.e. there are $c_1, \dots, c_n \in S$ such that $S = R[c_1, \dots, c_n]$). Then S is called *finitely generated R -algebra* (or *affine R -algebra*). If R is noetherian, then so is S .

Proof. We consider the valuation homomorphism

$$\begin{aligned} \Phi_{c_1, \dots, c_n}^{X_1, \dots, X_n}: R[X_1, \dots, X_n] &\rightarrow R[c_1, \dots, c_n] = S \\ X_i &\mapsto c_i. \end{aligned}$$

By Theorem 3.19, $R[X_1, \dots, X_n]$ is noetherian, and thus S is noetherian by 2.37. \square

Definition 3.21. Let $I \triangleleft R$ be an ideal. The *radical* of I is

$$\sqrt{I} = \{x \in R \mid \exists n \in \mathbb{N}: x^n \in I\}.$$

Obviously $I \subseteq \sqrt{I} \subseteq R$, and I is called *radical ideal* if $I = \sqrt{I}$.

Proposition 3.22. Let $I, J \triangleleft R$. Then:

1. If $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.
2. $\sqrt{I} = \sqrt{\sqrt{I}} = \sqrt{I^n}$, for all $n \in \mathbb{N}$.
3. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

4. If $I \neq R$, then $\sqrt{I} \neq R$.
5. $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
6. If $I \in \text{Spec}(R)$, then $I = \sqrt{I}$.

Proof.

1. Trivial.
2. We have $I^n \subseteq I \subseteq \sqrt{I}$, thus by point (1) we get $\sqrt{I^n} \subseteq \sqrt{I} \subseteq \sqrt{\sqrt{I}}$. If $x \in \sqrt{\sqrt{I}}$, then there is an $l \in \mathbb{N}$ with $x^l \in \sqrt{I}$, and so there is a $k \in \mathbb{N}$ with $x^{kl} \in I$. Thus $x^{kln} \in I^n$ and $x \in \sqrt{I^n}$.
3. We have $IJ \subseteq I \cap J \subseteq \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{\sqrt{I} \cap \sqrt{J}}$. If $x \in \sqrt{\sqrt{I} \cap \sqrt{J}}$, then there is an $m \in \mathbb{N}$ with $x^m \in I$ and $x^m \in J$, thus $x^{2m} \in IJ$, i.e. $x \in \sqrt{IJ}$.
4. If $\sqrt{I} = R$, then there are $x \in I$ and $m \in \mathbb{N}$ such that $x^m = 1$, and thus $x \in I \cap R^\times$, i.e. $I = R$.
5. We have $I + J \subseteq \sqrt{I} + \sqrt{J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$. If $x \in \sqrt{\sqrt{I} + \sqrt{J}}$, then there are $n, m \in \mathbb{N}$ such that $x^m = a + b$ with $a^n \in I$ and $b^n \in J$. It follows that

$$x^{2mn} = (a + b)^{2n} = \sum_{\nu=0}^{2n} \binom{2n}{\nu} a^\nu b^{2n-\nu} \in I + J.$$

6. Trivial.

□

Proposition 3.23. Let $I \triangleleft R$ be an ideal.

1. $\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathcal{V}(I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathbb{P}(I)} \mathfrak{p}$.
2. If $J \triangleleft R$ is finitely generated and $J \subseteq \sqrt{I}$, then there is an $m \in \mathbb{N}$ such that $J^m \subseteq I$.
3. $\sqrt{0} = \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{m} \in \text{max}(R)} \mathfrak{m} = \mathcal{J}(R)$. $\sqrt{0}$ is called *nilradical* of R .

Proof.

1. We will show

$$\sqrt{I} \stackrel{(i)}{\subseteq} \bigcap_{\mathfrak{p} \in \mathcal{V}(I)} \mathfrak{p} \stackrel{(ii)}{\subseteq} \bigcap_{\mathfrak{p} \in \mathbb{P}(I)} \mathfrak{p} \stackrel{(iii)}{\subseteq} \sqrt{I}.$$

- (i) If $x \in \sqrt{I}$ and $\mathfrak{p} \in \mathcal{V}(I)$, then there is an $m \in \mathbb{N}$ with $x^m \in I \subseteq \mathfrak{p}$, and thus $x \in \mathfrak{p}$.
- (ii) Trivial.
- (iii) Let $a \in R \setminus \sqrt{I}$. We claim that there is a $\mathfrak{p}_0 \in \mathbb{P}(I)$ such that $a \notin \mathfrak{p}_0$. The set $S = \{a^n \mid n \in \mathbb{N}_0\}$ is multiplicatively closed with $S \cap I = \emptyset$. Then it follows

$$I \in \Omega = \{J \triangleleft R \mid J \cap S = \emptyset, I \subseteq J\}.$$

By Krull's Existence Theorem, Ω has a maximal element $\mathfrak{p} \in \text{Spec}(R)$.

By Theorem 3.18(1), there is a $\mathfrak{p}_0 \in \mathbb{P}(I)$ such that $I \subseteq \mathfrak{p}_0 \subseteq \mathfrak{p}$.

- 2. Let $J = {}_R\langle x_1, \dots, x_k \rangle$. By hypothesis there is an $n \in \mathbb{N}$ with $x_i^n \in I$ for all $i \in [1, k]$. If $a \in J$, then $a = \sum_{i=1}^k \lambda_i x_i$ with $\lambda_1, \dots, \lambda_k \in R$, and it is easy to see that writing a^{nk} explicitly, every addend contains at least one factor x_i^h with $h \geq n$. Hence $a^{nk} \in I$.
- 3. This follows from (1), since $\mathcal{V}(\{0\}) = \text{Spec}(R)$ and since every maximal ideal is prime.

□

3.4 Hilbert's Nullstellensatz.

Definition 3.24. Let $K \subseteq L$ be fields and $n \in \mathbb{N}$.

- 1. Let $Z \subseteq K[X_1, \dots, X_n]$. We denote with $\mathcal{V}_L(Z)$ the set

$$\mathcal{V}_L(Z) := \{\mathbf{x} \in L^n \mid \forall f \in Z: f(\mathbf{x}) = 0\} \subseteq L^n,$$

which is the set of solutions of the system of polynomial equations $f(\mathbf{x}) = 0$ for all $f \in Z$ in L^n .

- 2. A subset $V \subseteq L^n$ is called (*affine, algebraic*) K -variety if there are $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ such that V is the set of solutions of the system

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

in L^n , i.e. if $V = \mathcal{V}_L(\{f_1, \dots, f_m\})$.

Theorem 3.25. Let $K \subseteq L$ be fields and $Z \subseteq K[X_1, \dots, X_n]$. We have:

- $\mathcal{V}_L(Z) = \mathcal{V}_L(K[\mathbf{X}]\langle Z \rangle)$.
- There is a finite subset $E \subseteq Z$ such that $\mathcal{V}_L(E) = \mathcal{V}_L(Z)$.

Proof.

1. The inclusion “ \supseteq ” is trivial. Let’s show “ \subseteq ”. Let $\mathbf{x} \in \mathcal{V}_L(Z)$. If $f \in \langle Z \rangle$, then $f = \sum_{i=1}^k g_i h_i$ with $g_i \in K[\mathbf{X}]$ and $h_i \in Z$ for all $i \in [1, k]$. Then $f(\mathbf{x}) = \sum_{i=1}^k g_i(\mathbf{x}) h_i(\mathbf{x}) = 0$, and thus $\mathbf{x} \in \mathcal{V}_L(\langle Z \rangle)$.
2. By theorem 3.19, $K[\mathbf{X}]$ is noetherian and thus $\langle Z \rangle$ is finitely generated. By the remark after Definition 2.3, there is a finite $E \subseteq Z$ with $\langle E \rangle = \langle Z \rangle$. Then

$$\mathcal{V}_L(Z) = \mathcal{V}_L(\langle Z \rangle) = \mathcal{V}_L(\langle E \rangle) = \mathcal{V}_L(E).$$

□

Definition 3.26. Let $K \subseteq L$ be fields and $V \subseteq L^n$. Then

$$\mathcal{J}(V) = \{f \in K[\mathbf{X}] \mid f(\mathbf{a}) = 0 \text{ for all } \mathbf{a} \in V\} \triangleleft K[\mathbf{X}]$$

is called *vanishing ideal of V*.

Theorem 3.27 (Field-theoretic version of Hilbert’s Nullstellensatz). Let K be a field and $A = K[x_1, \dots, x_n]$ a finitely generated K -algebra. Then the embedding $K \hookrightarrow \overline{K}$ (\overline{K} is the algebraic closure of K) can be lifted to a ring K -homomorphism $A \rightarrow \overline{K}$. If A is a field, then A/K is an algebraic field extension.

Proof. Bosch (Algebra II, Paragraph 39). □

Lemma 3.28. Let K be a field and $a_1, \dots, a_n \in K$. Then:

1. $\mathfrak{m} = \langle X_1 - a_1, \dots, X_n - a_n \rangle \subseteq K[\mathbf{X}]$ is a maximal ideal such that $\mathcal{V}_K(\mathfrak{m}) = \{\mathbf{a}\} \subseteq K^n$ and $\mathcal{J}(\{\mathbf{a}\}) = \mathfrak{m}$.
2. If K is algebraically closed and $\mathfrak{m} \triangleleft K[\mathbf{X}]$ is a maximal ideal, then there are $b_1, \dots, b_n \in K$ such that $\mathfrak{m} = \langle X_1 - b_1, \dots, X_n - b_n \rangle$.

Proof.

1. We consider the valuation homomorphism

$$\begin{aligned} \varphi &:= \Phi_{a_1, \dots, a_n}^{X_1, \dots, X_n} : K[X_1, \dots, X_n] \rightarrow K \\ &X_i \mapsto a_i. \end{aligned}$$

Then $K[\mathbf{X}]/\ker(\varphi) \simeq K$, thus $\ker(\varphi) \in \max(K[\mathbf{X}])$ and $\mathfrak{m} := \langle X_1 - a_1, \dots, X_n - a_n \rangle \subseteq \ker(\varphi)$. We want to show that equality holds, and so $\mathfrak{m} \in \max(K[\mathbf{X}])$. Every $f \in K[\mathbf{X}]$ has a unique representation of the form

$$f = \sum_{\mathbf{m}=(m_1, \dots, m_n) \in \mathbb{N}_0^n} b_{\mathbf{m}} \prod_{i=1}^n (X_i - a_i)^{m_i}. \quad (\text{Taylor series})$$

Hence, if $f \in \ker(\varphi)$, then $0 = f(\mathbf{a}) = b_{\mathbf{0}}$, and thus $f \in \langle X_1 - a_1, \dots, X_n - a_n \rangle$. Obviously $\mathcal{V}_K(\mathfrak{m}) = \{\mathbf{a}\}$. Furthermore, $\mathfrak{m} \subseteq \mathcal{J}(\{\mathbf{a}\}) \neq K[\mathbf{X}]$ and thus $\mathfrak{m} = \mathcal{J}(\{\mathbf{a}\})$ by maximality.

2. Let K be algebraically closed and $\mathfrak{m} \triangleleft K[\mathbf{X}]$ maximal. By Theorem 3.27, there is a K -homomorphism $K[\mathbf{X}]/\mathfrak{m} \rightarrow K$ (???), which then is an isomorphism (???). Thus there is a K -epimorphism $\varphi : K[\mathbf{X}] \rightarrow K$ with $\ker(\varphi) = \mathfrak{m}$. Of course

$$\langle X_1 - \varphi(X_1), \dots, X_n - \varphi(X_n) \rangle \subseteq \ker(\varphi),$$

and since $\langle X_1 - \varphi(X_1), \dots, X_n - \varphi(X_n) \rangle$ is maximal by (1), the statement follows. □

3.29. Hilbert's Nullstellensatz. Let L/K be a field extension, L algebraically closed, $n \in \mathbb{N}$ and $R = K[\mathbf{X}]$. The following statements hold:

1. If $I \triangleleft R$ with $I \neq R$, then $\mathcal{V}_L(I) \neq \emptyset$.
2. If $I \triangleleft R$, then $\mathcal{J}(\mathcal{V}_L(I)) = \sqrt{I}$. The maps

$$\begin{aligned} \{K\text{-variety}, V \subseteq L^n\} &\rightarrow \{\text{radical ideals of } R\} \\ V &\mapsto \mathcal{J}(V) \\ \mathcal{V}_L(I) &\mapsto I \end{aligned}$$

are bijective and are each other's inverse.

Proof.

1. Special case: $L = K$. Since $I \neq R$ there is a maximal ideal $\mathfrak{m} = \langle X_1 - a_1, \dots, X_n - a_n \rangle$ with $I \subseteq \mathfrak{m}$, and thus $\{\mathbf{a}\} = \mathcal{V}_L(\mathfrak{m}) \subseteq \mathcal{V}_L(I)$.
General case: Let $\mathfrak{m} \in \max(K[\mathbf{X}])$ with $I \subseteq \mathfrak{m}$. Then $A := K[\mathbf{X}]/\mathfrak{m}$ is a field. The function

$$\begin{aligned} \Phi : K[\mathbf{X}] &\rightarrow K[\mathbf{X}]/\mathfrak{m} \\ X_i &\mapsto \xi_i := X_i + \mathfrak{m} \end{aligned}$$

is trivially a ring K -epimorphism, and thus $A = K[\xi_1, \dots, \xi_n]$ is a finitely generated K -algebra. By 3.27, A/K is algebraic and there is a K -homomorphism $\varphi : A \rightarrow \bar{K}$. Since L is algebraically closed, $\bar{K} \subseteq L$ (??? siamo sicuri di sta implicazione?), and so we can write $\varphi : A \rightarrow L$. Thus

$$\left(\varphi(\xi_1), \dots, \varphi(\xi_n)\right) \in L^n$$

is a root of \mathfrak{m} , and thus of I . Indeed, if $f \in \mathfrak{m}$ then

$$\begin{aligned} f\left(\varphi(\xi_1), \dots, \varphi(\xi_n)\right) &= \varphi\left(f(\xi_1, \dots, \xi_n)\right) = \varphi\left(f(\Phi(X_1), \dots, \Phi(X_n))\right) = \\ &= \varphi\left(\Phi(f(X_1, \dots, X_n))\right) = \varphi(0) = 0, \end{aligned}$$

where the first and the third equality hold because φ and Φ respectively are ring homomorphisms and f is a polynomial, and the fourth follows because $f \in \mathfrak{m}$ and Φ is the projection on the quotient).

2. Claim 1: Let $V \subseteq L^n$ be a subset. Then $\mathcal{J}(V)$ is a radical ideal.

Proof: If $f \in K[\mathbf{X}]$ with $f^n \in \mathcal{J}(V)$, then $f^n(\mathbf{a}) = 0$ for all $\mathbf{a} \in V$, and thus $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in V$, i.e. $f \in \mathcal{J}(V)$. ■

Claim 2: $\mathcal{V}_L(\mathcal{J}(\mathfrak{U})) = \mathfrak{U}$ for all K -varieties $\mathfrak{U} \in L^n$.

Proof: Let $\mathfrak{U} := \mathcal{V}_L(\mathfrak{g})$ with $\mathfrak{g} \subseteq K[X]$. By Theorem 3.25 we can assume w.l.o.g. $\mathfrak{g} \triangleleft K[\mathbf{X}]$. We need to show $\mathcal{V}_L(\mathcal{J}(\mathcal{V}_L(\mathfrak{g}))) = \mathcal{V}_L(\mathfrak{g})$.

The inclusion “ \supseteq ” is immediate, since the polynomials in $\mathcal{J}(\mathcal{V}_L(\mathfrak{g}))$ are zero on $\mathcal{V}_L(\mathfrak{g})$.

For the inclusion “ \subseteq ”, observe that all the polynomials of \mathfrak{g} are zero on $\mathcal{V}_L(\mathfrak{g})$, i.e. $\mathfrak{g} \subseteq \mathcal{J}(\mathcal{V}_L(\mathfrak{g}))$, and thus $\mathcal{V}_L(\mathfrak{g}) \supseteq \mathcal{V}_L(\mathcal{J}(\mathcal{V}_L(\mathfrak{g})))$. ■

Claim 3: $\mathcal{J}(\mathcal{V}_L(I)) = \sqrt{I}$.

Proof: “ \supseteq ” The polynomials of I are zero on $\mathcal{V}_L(I)$, i.e. $I \subseteq \mathcal{J}(\mathcal{V}_L(I))$, and thus $\sqrt{I} \subseteq \sqrt{\mathcal{J}(\mathcal{V}_L(I))} = \mathcal{J}(\mathcal{V}_L(I))$ by Claim 1.

“ \subseteq ” Let $0 \neq f \in \mathcal{J}(\mathcal{V}_L(I))$. Consider

$$\mathfrak{g} := \langle I, fT - 1 \rangle \triangleleft K[X_1, \dots, X_n, T] = K[\mathbf{X}, T].$$

We claim that $\mathcal{V}_L(\mathfrak{g}) = \emptyset$. Suppose to the contrary $(x_1, \dots, x_n, t) \in L^{n+1}$ is in $\mathcal{V}_L(\mathfrak{g})$. Then $(x_1, \dots, x_n) \in \mathcal{V}_L(I)$, and thus $f(x_1, \dots, x_n)t - 1 = -1 \neq 0$. But (x_1, \dots, x_n, t) must be a root of $fT - 1 \in K[\mathbf{X}, T]$, contradiction.

So $\mathcal{V}_L(\mathfrak{g}) = \emptyset$, and by point (1) follows that $\mathfrak{g} = K[\mathbf{X}, T]$. Hence there exist $f_1, \dots, f_s \in I$ and $p_1, \dots, p_{s+1} \in K[\mathbf{X}, T]$ such that

$$1 = \sum_{i=1}^s f_i p_i + p_{s+1}(fT - 1).$$

We consider the ring $K[\mathbf{X}]$ -homomorphism

$$\begin{aligned}\varphi &:= \Phi_{(X_1, \dots, X_n, \frac{1}{f})}^{(X_1, \dots, X_n, T)} : K[\mathbf{X}, T] \rightarrow K(X_1, \dots, X_n) \\ X_i &\mapsto X_i \\ T &\mapsto \frac{1}{f}.\end{aligned}$$

Then

$$1 = \sum_{i=1}^s \varphi(p_i) f_i,$$

Obviously we have $\varphi(p_i) = \frac{q_i}{f^{m_i}}$ for some $q_i \in K[\mathbf{X}]$, $m_i \in \mathbb{N}$. Therefore, setting $m := \max\{m_1, \dots, m_s\}$ we get

$$f^m \in {}_{K[X]}\langle f_1, \dots, f_s \rangle \subseteq I,$$

i.e. $f \in \sqrt{I}$. ■

We showed everything we set out to prove. □

Chapter 4

Ring extensions

4.1 Algebras

Definition 4.1. Let R be a commutative ring. An (associative, unitary) R -algebra is an R -module A together with a multiplication $\cdot : A \times A \rightarrow A$ such that:

- (A1) $(A, +, \cdot)$ is a (not necessarily commutative) ring;
- (A2) For all $\lambda \in R$ and all $a, b \in A$, $\lambda(ab) = a(\lambda b)$.

If $(A, +, \cdot)$ is a commutative ring, then A is called a commutative R -algebra.

Remarks and examples.

1. For every $n \in \mathbb{N}$, $M_n(R)$ is an R -algebra and $R[X_1, \dots, X_n]$ is a commutative R -algebra.
2. If A is an R -algebra, then $\varepsilon : R \rightarrow A$, $\lambda \mapsto \lambda 1_A$ is a ring homomorphism, and for all $\lambda \in R$ and $a \in A$, $\varepsilon(\lambda)a = a\varepsilon(\lambda)$.

Proof. For all $\lambda, \mu \in R$ and $a \in A$, we have:

$$\varepsilon(\lambda\mu) = (\lambda\mu)1_A = \lambda(\mu 1_A) = \lambda[1_A(\mu 1_A)] = (\lambda 1_A)(\mu 1_A) = \varepsilon(\lambda)\varepsilon(\mu)$$

and

$$\varepsilon(\lambda)a = (\lambda 1_A)a = \lambda(1_A a) = \lambda(a 1_A) = a(\lambda 1_A) = a\varepsilon(\lambda).$$

□

3. Conversely, let A be a ring and $\varepsilon : R \rightarrow A$ a ring homomorphism such that $\varepsilon(\lambda)a = a\varepsilon(\lambda)$ for all $\lambda \in R$ and all $a \in A$. Then (check details) A is an

R -module and an R -algebra. Then ε is called the *structural homomorphism* of the R -algebra A , and also $\varepsilon : R \rightarrow A$ is called an R -algebra.

In particular, every commutative overring $S \supseteq R$ and every epimorphic image of R is an R -algebra.

4. Let $\varepsilon_1 : R \rightarrow A_1$ and $\varepsilon_2 : R \rightarrow A_2$ be the structural homomorphisms of A_1 and A_2 respectively. A ring homomorphism $f : A_1 \rightarrow A_2$ is an *R -algebra homomorphism* if $f \circ \varepsilon_1 = \varepsilon_2$ (or, equivalently, if f is a module homomorphism). Suppose $A_1 \supseteq R$ and $A_2 \supseteq R$ are commutative overring and $f : A_1 \rightarrow A_2$ is a ring homomorphism. Then f is an R -algebra homomorphism if and only if $f|_R = \text{id}_R$.

Proof.

“ \Rightarrow ”: If $\lambda \in R$, then $f(\lambda) = f(\lambda 1) = \lambda f(1) = \lambda 1 = \lambda$.

“ \Leftarrow ”: If $\lambda \in R$ and $a \in A$, then $f(\lambda a) = f(\lambda)f(a) = \lambda f(a)$. □

5. If R is a ring, then there is exactly one ring homomorphism $\varepsilon : \mathbb{Z} \rightarrow R$ (namely, $\varepsilon(m) = m1_R$). Thus R is a \mathbb{Z} -algebra.

More notations and conventions.

1. Let $0 \neq R \subseteq S$ commutative rings with S an overring. Then $S \supseteq R$, indicated also S/R , is called a *ring extension*.

For all $\mathfrak{p} \in \text{Spec}(S)$ we have $\mathfrak{p} \cap R \in \text{Spec}(R)$.

For any $C \subseteq S$, let $[C] = \{c_1 \cdots c_n \mid n \in \mathbb{N}_0, c_1, \dots, c_n \in C\}$ be the semigroup of S generated by C , and $R[C] = {}_R\langle [C] \rangle \subseteq S$. Then $R[C]$ is the smallest subring of S containing $R \cup C$.

If $S' = R[C]$ and if $\varphi_1, \varphi_2 : S \rightarrow S'$ are ring homomorphism with $\varphi_1|_{R \cup C} = \varphi_2|_{R \cup C}$, then $\varphi_1 = \varphi_2$.

2. Let R be a commutative ring, A a commutative R -algebra and $\varepsilon : R \rightarrow A$ the structural homomorphism. Then A is called a *finitely generated R -algebra* (or an *R -algebra of finite type*, or an *affine R -algebra*) if one of the following equivalent conditions is satisfied:

- There exist an $n \in \mathbb{N}$ and an epimorphism $R[X_1, \dots, X_n] \rightarrow A$.
- There exist $n \in \mathbb{N}$, $x_1, \dots, x_n \in A$ with $A = \varepsilon[R][x_1, \dots, x_n]$, i.e. A is the smallest subring of A which contains $\varepsilon[R] \cup \{x_1, \dots, x_n\}$.

4.2 Integral ring extensions and the Theorem of Cohen-Seidenberg.

Definition 4.2. Let $R \subseteq S$ be a ring extension.

1. An element $x \in S$ is called *integral over R* (*integral/ R*) if there is a monic polynomial $0 \neq f \in R[X]$ with $f(x) = 0$, i.e. there are $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in R$ such that $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$. The latter is called an *integral equation of x/R* .
2. The *integral closure of R in S* is $\text{cl}_S(R) := \{x \in S \mid x \text{ is integral}/R\}$.
3. A subset $S' \subseteq S$ is called *integral/ R* if $S' \subseteq \text{cl}_S(R)$.
4. R is called *integrally closed in S* if $\text{cl}_S(R) = R$.
5. If R is a domain with $\mathfrak{q}(R) = K$, then R is called *integrally closed* if $\text{cl}_K(R) = R$.

Remarks and examples.

1. Let $R \subseteq S$ be fields and $x \in S$. Then x is integral/ R iff x is algebraic/ R .
2. Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the algebraic closure of \mathbb{Q} . This is called the *field of algebraic numbers*. $\overline{\mathbb{Z}} = \text{cl}_{\overline{\mathbb{Q}}}(\mathbb{Z}) = \text{cl}_{\mathbb{C}}(\mathbb{Z})$ is the *ring of all algebraic integers*.
3. Every field is trivially integrally closed by definition.

Theorem 4.3. Let $R \subseteq S$ be a ring extension and $x \in S$. The following are equivalent:

- (a) x is integral/ R .
- (b) $R[x]$ is a finitely generated R -module.
- (c) There is a subring S' with $R[x] \subseteq S' \subseteq S$ such that S' is a finitely generated R -module.
- (d) There is an $R[x]$ -module M such that $\text{Ann}_{R[x]}(M) = 0$ and M is a finitely generated R -module.

Proof.

(a) \Rightarrow (b) Let $n \in \mathbb{N}$, $a_{n-1}, \dots, a_0 \in R$ such that $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$. By definition we have

$$R[x] = \left\{ \sum_{j=0}^k c_j x^j \mid k \in \mathbb{N}_0, c_0, \dots, c_k \in R \right\}$$

and hence $R[x] = {}_R\langle \{x^j \mid j \in \mathbb{N}_0\} \rangle$.

Claim: $R[x] = {}_R\langle \{x^j \mid j \in [0, n-1]\} \rangle$.

Proof: The inclusion “ \supseteq ” is trivial. We want to prove “ \subseteq ”. It is sufficient to show that $x^k \in {}_R\langle \{x^j \mid j \in [0, n-1]\} \rangle$ for every $k \in \mathbb{N}_0$. We proceed by induction. If $k \leq n-1$ the assertion is clearly true. Let $k \geq n$ and suppose $\{x^0, \dots, x^{k-1}\} \subseteq {}_R\langle \{x^j \mid j \in [0, n-1]\} \rangle$. Then

$$\begin{aligned} x^k &= x^{k-n} x^n = x^{k-n} (-a_{n-1}x^{n-1} - \dots - a_0) = \\ &\quad -a_{n-1}x^{k-1} - \dots - a_0x^{k-n} \in {}_R\langle \{x^j \mid j \in [0, n-1]\} \rangle. \end{aligned}$$

■

(b) \Rightarrow (c) $S' := R[x]$ has the required property.

(c) \Rightarrow (d) $M := S'$ has the required property, because if $a \in R[x]$ with $aS' = \{0_{S'}\}$, then $a1_{S'} = 0_{S'}$, and hence $a = 0$.

(d) \Rightarrow (a) By hypothesis $M = {}_R\langle m_1, \dots, m_n \rangle$, and M is also an $R[x]$ -module. Thus $xM \subseteq M$. Therefore, for all $i \in [1, n]$ there are $r_{i,1}, \dots, r_{i,n} \in R$ such that

$$xm_i = \sum_{j=1}^n r_{i,j} m_j$$

and hence

$$\sum_{j=1}^n (r_{i,j} - \delta_{i,j}x) m_j = 0.$$

Now define $A := (a_{i,j})_{i,j} \in M_n(R)$ with $a_{i,j} := r_{i,j} - \delta_{i,j}x$. Then

$$A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

and hence

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = A^\# A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \underbrace{\det(A)}_{\in R} I \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \det(A)m_1 \\ \vdots \\ \det(A)m_n \end{pmatrix}$$

where $A^\#$ is the adjugate matrix¹ of A . So $\det(A)m_i = 0$ for all $i \in [1, n]$, i.e. $\det(A) \in \text{Ann}_R(M)$. Since $\text{Ann}_{R[x]}(M) = 0$ by hypothesis, we get $\det(A) = 0$. Thus there are $w_0, \dots, w_{n-1} \in R$ such that

$$0 = \det(A) = (-1)^n x^n + w_{n-1}x^{n-1} + \dots + w_0,$$

which is an integral equation for x . □

Lemma 4.4. Let $R \subseteq S$ be a ring extension with S a finitely generated R -module. If M is a finitely generated S -module, then M is a finitely generated R -module.

Proof. Let $M = {}_S\langle x_1, \dots, x_n \rangle$ and $S = {}_R\langle a_1, \dots, a_m \rangle$. We claim that

$$M = {}_R\langle a_j x_i \mid j \in [1, m], i \in [1, n] \rangle.$$

Let $x \in M$. Then there are $s_1, \dots, s_n \in S$ such that $x = \sum_{i=1}^n s_i x_i$. For all $i \in [1, n]$ there are $\lambda_{i,1}, \dots, \lambda_{i,m} \in R$ such that $s_i = \sum_{j=1}^m \lambda_{i,j} a_j$. Thus

$$x = \sum_{i=1}^n s_i x_i = \sum_{i=1}^n \left(\sum_{j=1}^m \lambda_{i,j} a_j \right) x_i = \sum_{i=1}^n \sum_{j=1}^m \lambda_{i,j} (a_j x_i).$$

□

Examples.

1. $M := \mathbb{C}^n$, $R := \mathbb{R} \subseteq \mathbb{C} =: S$.
2. Field extension: $K \subseteq L \subseteq M$.

Corollary 4.5. Let $R \subseteq S$ be a ring extension and $x_1, \dots, x_n \in S$ with $S = R[x_1, \dots, x_n]$. The following are equivalent:

- (a) $\{x_1, \dots, x_n\} \subseteq \text{cl}_S(R)$.
- (b) S is a finitely generated R -module.
- (c) S is integral over R .

Proof.

¹If B is a matrix, the *adjugate matrix* $B^\#$ of B is defined in such a way that $BB^\# = \det(B)I$, and thanks to Laplace's formula for the determinant of a square matrix, we have $BB^\# = B^\#B$. See http://en.wikipedia.org/wiki/Adjugate_matrix.

²Observe that the x 's appear only on the diagonal, and all of them with coefficient 1.

- (a) \Rightarrow (b) We proceed by induction on n . For $n = 1$, this is the statement of Theorem 4.3. Let $n \geq 2$. By induction hypothesis, $S' = R[x_1, \dots, x_{n-1}]$ is a finitely generated R -module. Since x_n is integral/ R , x_n is integral/ S' . Again by induction hypothesis, $S'[x_n] = R[x_1, \dots, x_n]$ is a finitely generated S' -module, and thus it is a finitely generated R -module by Lemma 4.4.
- (b) \Rightarrow (c) By Theorem 4.3 with $S' := R[x_1, \dots, x_n]$, every $x \in S$ is integral/ R .
- (c) \Rightarrow (a) By definition. \square

Corollary 4.6. Let $R \subseteq S$ be a ring extension.

1. Let $S \subseteq T$ be a ring extension, and suppose that S is integral/ R . Then
 - (a) If $x \in T$ is integral/ S , then x is integral/ R .
 - (b) If T is integral/ S , then T is integral/ R .
2. We have $R \subseteq \text{cl}_S(R) \subseteq S$, and $\text{cl}_S(R)$ is a ring which is integrally closed in S .

Proof.

1. It suffices to prove (a). Let $x \in T$ be integral/ S . Then there exist $n \in \mathbb{N}_0$, $b_0, \dots, b_{n-1} \in S$ such that $x^n + b_{n-1}x^{n-1} + \dots + b_0 = 0$. Thus x is integral over $S' := R[b_0, \dots, b_{n-1}]$, and therefore $S'[x]$ is a finitely generated S' -module by Theorem 4.3. Since b_0, \dots, b_{n-1} are integral/ R , by Corollary 4.5 we obtain that S' is a finitely generated R -module. Hence $S'[x]$ is a finitely generated R -module, and finally x is integral/ R by Theorem 4.3(c).
2. (i) We assert that $\text{cl}_S(R) \subseteq S$ is a subring.
Let $x, y \in \text{cl}_S(R)$. We have to show that $x - y$ and xy are integral/ R . This follows by considering $R[x, y]$ (which of course contains $x - y$ and xy) and applying Corollary 4.5.
- (ii) We want to prove that $\text{cl}_S(R)$ is integrally closed in S . Let $x \in S$ be integral/ $\text{cl}_S(R)$. Since $\text{cl}_S(R)$ is integral/ R , by point (1) we have that x is integral/ R , i.e. $x \in \text{cl}_S(R)$.

\square

Theorem 4.7. Let R be an integrally closed domain with $\mathfrak{q}(R) = K$, L/K a field extension, $x \in L$ algebraic/ K and $f \in K[X]$ the minimal polynomial of x over K . Then x is integral/ R if and only if $f \in R[X]$.

Proof. The implication “ \Leftarrow ” is obvious. We want to show “ \Rightarrow ”. Let N/L be a splitting field of f over L . So

$$f = \prod_{i=1}^n (X - x_i) \quad \text{with } x_1, \dots, x_n \in N.$$

We assume w.l.o.g. $x = x_1$. Then, for all $i \in [1, n]$, there is a K -isomorphism of rings

$$\varphi_i : K[x] \rightarrow K[x_i] \subseteq N, \quad \varphi_i(x) = x_i.$$

By hypothesis, there exist $a_0, \dots, a_{d-1} \in R$ such that $x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0 = 0$. Therefore

$$\varphi_i(x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0) = x_i^d + a_{d-1}x_i^{d-1} + \dots + a_1x_i + a_0 = 0,$$

i.e. x_i is integral/ R . So the coefficients of f are integral/ R , because we proved in 4.6 that sums and products of integral elements are integral. But the coefficients are clearly also in K , by definition of f . Since R is integrally closed, this means that they are in R , i.e. $f \in R[X]$. \square

Corollary 4.8. Let R be an integrally closed domain, $K = \mathbf{q}(R)$, $f \in R[X] \setminus R$ monic and $g, h \in K[X] \setminus K$ with $f = gh$. Then $g, h \in R[X]$. In particular, if f is irreducible/ R , then f is irreducible/ K .

Proof. Claim: If $p \in K[X]$ is monic and irreducible with $p|f$ in $K[X]$, then $p \in R[X]$. Proof: Let L/K be a field extension with $\alpha \in L$ and $p(\alpha) = 0$. Then p is the minimal polynomial of α over K , and since $p|f$ we have obtain $f(\alpha) = 0$. Therefore α is integral/ R , and hence $p \in R[X]$ by Theorem 4.7. \blacksquare
Since $K[X]$ is a UFD, the main statement follows. \square

Definition 4.9. Let $0 \neq R$ be a commutative ring and $\mathfrak{g} \in \text{Spec}(R)$. Then

$$h(\mathfrak{g}) := \sup\{l \in \mathbb{N}_0 \mid \text{there are prime ideals } \mathfrak{g} = \mathfrak{g}_0 \supsetneq \dots \supsetneq \mathfrak{g}_l\}$$

is called the *height of* \mathfrak{g} , and

$$\dim(R) := \sup\{h(\mathfrak{g}) \mid \mathfrak{g} \in \text{Spec}(R)\}$$

is called the (Krull) *dimension of* R .

Remarks.

1. R is a domain if and only if $0 \in \text{Spec}(R)$. R is a field if and only if $\dim(R) = 0$.

2. (Krull's Principal Ideal Theorem). Let R be noetherian, $x \in R^\circ$ and $\mathfrak{g} \in P(xR)$, where $P(xR)$ is the family of minimal prime ideals lying in xR . Then $\text{h}(\mathfrak{g}) \leq 1$. In particular, if R is a PID, then $\dim(R) = 1$.

4.10. Cohen-Seidenberg Theorem. Let $R \subseteq S$ be an integral ring extension. The following hold:

1. (Incomparability) Let $\mathfrak{p} \in \text{Spec}(S)$ and $\mathfrak{a} \triangleleft S$ with $\mathfrak{p} \subseteq \mathfrak{a}$ and $\mathfrak{p} \cap R = \mathfrak{a} \cap R$. Then $\mathfrak{p} = \mathfrak{a}$.
2. (Lying over) For every $\mathfrak{g} \in \text{Spec}(R)$ and $\mathfrak{a} \triangleleft S$ with $\mathfrak{a} \cap R \subseteq \mathfrak{g}$ there is a $\mathfrak{p} \in \text{Spec}(S)$ such that $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap R = \mathfrak{g}$. In particular, the map $\text{Spec}(S) \rightarrow \text{Spec}(R)$, $\mathfrak{p} \mapsto \mathfrak{p} \cap R$, is surjective.
3. (Going up) Let $\mathfrak{g}_0, \mathfrak{g} \in \text{Spec}(R)$ and $\mathfrak{p}_0 \in \text{Spec}(S)$ such that $\mathfrak{p}_0 \cap R = \mathfrak{g}_0 \subseteq \mathfrak{g}$. Then there is a $\mathfrak{p} \in \text{Spec}(S)$ such that $\mathfrak{p}_0 \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap R = \mathfrak{g}$.
4. $\max(S) = \{\mathfrak{p} \in \text{Spec}(S) \mid \mathfrak{p} \cap R \in \max(R)\}$. In particular, for every $\mathfrak{m} \in \max(R)$ there is a $\mathfrak{p} \in \max(S)$ such that $\mathfrak{p} \cap R = \mathfrak{m}$.
5. $S^\times \cap R = R^\times$. In particular, if S is a field, then R is a field.
6. $\dim(R) = \dim(S)$. Hence, if S is a domain, then S is a field if and only if R is a field.

Proof.

1. Let $x \in \mathfrak{a}$. We pick a minimal $n \in \mathbb{N}$ with the following property: there exist $a_0, \dots, a_{n-1} \in R$ with

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathfrak{p}.$$

Observe that such an n must exist since x is integral/ R , thus the property is satisfied at least by an integral equation for x over R .

Then there is a $p \in \mathfrak{p}$ such that

$$a_0 = p - x(x^{n-1} + \dots + a_1) \in \mathfrak{a} \cap R = \mathfrak{p} \cap R \subseteq \mathfrak{p},$$

hence $x(x^{n-1} + \dots + a_1) \in \mathfrak{p}$. By minimality $x^{n-1} + \dots + a_1 \notin \mathfrak{p}$, whereby $x \in \mathfrak{p}$.

2. Let $\mathfrak{g} \in \text{Spec}(R)$ and $\mathfrak{a} \triangleleft S$ with $\mathfrak{a} \cap R \subseteq \mathfrak{g}$. Then $R \setminus \mathfrak{g} \subseteq S$ is a multiplicatively closed subset with $\mathfrak{a} \cap (R \setminus \mathfrak{g}) = \emptyset$. By Theorem 3.1, the set $\{\mathfrak{c} \triangleleft S \mid \mathfrak{a} \subseteq \mathfrak{c}, \mathfrak{c} \cap (R \setminus \mathfrak{g}) = \emptyset\}$ has a maximal element $\mathfrak{p} \in \text{Spec}(S)$. Then $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap R \subseteq \mathfrak{g}$. If we can prove the following claim, we are done.

Claim: $\mathfrak{p} \cap R = \mathfrak{g}$.

Proof: Assume to the contrary that $\mathfrak{p} \cap R \subsetneq \mathfrak{g}$. Let $u \in \mathfrak{g} \setminus \mathfrak{p}$. By the maximality of \mathfrak{p} , it follows that $(\mathfrak{p} + uS) \cap (R \setminus \mathfrak{g}) \neq \emptyset$, so we pick $p \in \mathfrak{p}$ and $s \in S$ such that $x = p + us \in R \setminus \mathfrak{g}$. Take now

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

an integral equation of s over R . Then

$$u^n(s^n + a_{n-1}s^{n-1} + \dots + a_0) = (us)^n + a_{n-1}u(us)^{n-1} + \dots + a_1u^{n-1}(us) + a_0u^n = 0,$$

and since $us \equiv x \pmod{\mathfrak{p}}$ we get

$$x^n + a_{n-1}ux^{n-1} + \dots + a_1u^{n-1}x + a_0u^n \in \mathfrak{p} \cap R \subseteq \mathfrak{g}.$$

Since $u \in \mathfrak{g}$ we get $x^n \in \mathfrak{g}$, and thus $x \in \mathfrak{g}$, contradiction. ■

3. This follows immediately from (2) by defining $\mathfrak{a} = \mathfrak{p}_0$.
4. \supseteq Let $\mathfrak{p} \in \text{Spec}(S)$. If $\mathfrak{p} \notin \max(S)$, then by Corollary 3.2 there is an $\mathfrak{m} \in \max(S)$ with $\mathfrak{p} \subsetneq \mathfrak{m}$. Then point (1) implies that $\mathfrak{p} \cap R \subsetneq \mathfrak{m} \cap R$, and hence $\mathfrak{p} \cap R \notin \max(R)$.
 \subseteq If $\mathfrak{p} \cap R \notin \max(R)$, then there is an $\mathfrak{n} \in \max(R)$ with $\mathfrak{p} \cap R \subsetneq \mathfrak{n}$. By point (3), there is an $\mathfrak{m} \in \text{Spec}(S)$ with $\mathfrak{p} \subseteq \mathfrak{m}$ and $\mathfrak{m} \cap R = \mathfrak{n}$. Thus $\mathfrak{p} \subsetneq \mathfrak{m}$ and $\mathfrak{p} \notin \max(S)$.
5. Obviously, we have $R^\times \subseteq R \cap S^\times$. If $x \in R \setminus R^\times$, then there is an $\mathfrak{m} \in \max(R)$ with $x \in \mathfrak{m}$. By point (2), there is a $\mathfrak{p} \in \text{Spec}(S)$ such that $\mathfrak{m} \subseteq \mathfrak{p}$. Thus $x \in \mathfrak{p}$ and $x \notin S^\times$.
 If S is a field, then $R^\times = S^\times \cap R = S^\circ \cap R = R^\circ$, and hence R is a field.
6. Let $\mathfrak{g}_0 \subsetneq \mathfrak{g}_1 \subsetneq \dots \subsetneq \mathfrak{g}_n$ be a sequence in $\text{Spec}(R)$. By point (2), there is a $\mathfrak{p}_0 \in \text{Spec}(S)$ such that $\mathfrak{p}_0 \cap R = \mathfrak{g}_0$. Applying point (2) repeatedly, we obtain a sequence $\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_n$ in $\text{Spec}(S)$ with $\mathfrak{p}_i \cap R = \mathfrak{g}_i$ for all $i \in [1, n]$. Thus $\dim(S) \geq \dim(R)$. Conversely, if $\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_n$ is a sequence in $\text{Spec}(S)$, then $\mathfrak{p}_0 \cap R \subsetneq \dots \subsetneq \mathfrak{p}_n \cap R$ by point (1), and hence $\dim(S) \leq \dim(R)$.
 In particular, if S is a domain, then R is a domain, and thus $\dim(R) = \dim(S)$ implies that S is a field iff R is a field.

□

4.3 Rings of integers in algebraic number fields.

Definition 4.11. An *algebraic number field* is a finite field extension of \mathbb{Q} . If L/\mathbb{Q} is an algebraic number field, then

$$\mathcal{O}_L := \text{cl}_L(\mathbb{Z})$$

is called the *ring of integers of L* (or *principal order of L*).

Lemma 4.12. \mathcal{O}_L is an integrally closed, one-dimensional domain.

Proof. Since $\mathcal{O}_L \subseteq L$, \mathcal{O}_L is a domain. By Theorem 4.10, $\dim(\mathcal{O}_L) = \dim(\mathbb{Z}) = 1$. By Corollary 4.6, \mathcal{O}_L is integrally closed in L . It remains to show that $\mathfrak{q}(\mathcal{O}_L) = L$. Let $x \in L$. Since L/\mathbb{Q} is algebraic, there exist $a_n, \dots, a_0 \in \mathbb{Z}$ with

$$a_n x^n + \dots + a_0 = 0.$$

Multiplying by a_n^{n-1} we obtain that

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \dots + a_0 a_n^{n-1} = 0.$$

Thus $a_n x$ is integral/ \mathbb{Z} , which means $a_n x \in \mathcal{O}_L$. Hence $x \in \mathfrak{q}(\mathcal{O}_L)$. \square

Our goal is now to show that \mathcal{O}_L is noetherian.

Norm and trace.

Let K be a field, A a commutative K -algebra, and $\dim_K(A) = n$ (??? si intende la dimensione come modulo? se sì, l'abbiamo sempre indicata con $\text{rk} \dots$). For $\lambda \in A$, let $\mu_\lambda : A \rightarrow A$ be defined by

$$\mu_\lambda(a) = \lambda a.$$

Then $\mu_\lambda \in \text{End}_K(A)$, and we define

$$\begin{aligned} N_{A/K} : A &\rightarrow K & \text{and} & & \text{Tr}_{A/K} : A &\rightarrow K \\ \lambda &\mapsto N_{A/K}(\lambda) := \det(\mu_\lambda) & & & \lambda &\mapsto \text{Tr}_{A/K}(\lambda) := \text{Tr}(\mu_\lambda) \end{aligned}$$

Remark. Let $\mathbf{u} = (u_1, \dots, u_n)$ be a K -basis of A and let $\mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\lambda) \in M_n(K)$ be such that

$$(\lambda u_1, \dots, \lambda u_n) = (u_1, \dots, u_n) \mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\lambda).$$

Then $\det(\mu_\lambda) := \det(\mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\lambda))$ does not depend on \mathbf{u} , because if $\mathbf{u}' = \mathbf{u}S$, then for $\varphi \in \text{End}_K(A)$ we have

$$\mathcal{M}_{\mathbf{u}', \mathbf{u}'}(\varphi) = S^{-1} \mathcal{M}_{\mathbf{u}, \mathbf{u}}(\varphi) S.$$

Lemma 4.13. Let K be a field, A a commutative K -algebra with $\dim_K(A) = n$, $\alpha, \beta \in A$ and $\lambda \in K$. The following hold:

1. $N_{A/K}(\alpha\beta) = N_{A/K}(\alpha)N_{A/K}(\beta)$.
2. $N_{A/K}(\lambda) = \lambda^n$.
3. $\text{Tr}_{A/K}(\alpha + \beta) = \text{Tr}_{A/K}(\alpha) + \text{Tr}_{A/K}(\beta)$.
4. $\text{Tr}_{A/K}(\lambda\alpha) = \lambda \text{Tr}_{A/K}(\alpha)$.
5. $\text{Tr}_{A/K}(\lambda) = n\lambda$.

Proof.

1. Since $\mu_{\alpha\beta} = \mu_\alpha \circ \mu_\beta$, we get

$$N_{A/K}(\alpha\beta) = \det(\mu_{\alpha\beta}) = \det(\mu_\alpha \circ \mu_\beta) = \det(\mu_\alpha) \det(\mu_\beta) = N_{A/K}(\alpha)N_{A/K}(\beta).$$

- 2., 5. If $\mathbf{u} = (u_1, \dots, u_n)$ is a K -basis of A , then $\mu_\lambda(u_i) = \lambda u_i$ for all $i \in [1, n]$, and so $\mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\lambda) = \lambda I$.

- 3., 4. Observe that

$$\begin{aligned} \mathcal{M}_{\mathbf{u}, \mathbf{u}}: \text{End}_K(A) &\rightarrow M_n(K) \\ \varphi &\mapsto \mathcal{M}_{\mathbf{u}, \mathbf{u}}(\varphi) \end{aligned}$$

is a K -algebra isomorphism, i.e. $\mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_{\alpha+\beta}) = \mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\alpha + \mu_\beta) = \mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\alpha) + \mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\beta)$ and $\mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_{\lambda\alpha}) = \mathcal{M}_{\mathbf{u}, \mathbf{u}}(\lambda\mu_\alpha) = \lambda\mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\alpha)$, and we know that $\text{Tr}(A + B) = \text{Tr}(A) + \text{Tr}(B)$ and $\text{Tr}(\lambda A) = \lambda \text{Tr}(A)$.

□

For the rest of this Section, let L/K be a finite separable field extension of degree $[L : K] = n$, and let \bar{K} be an algebraically closed field with $K \subseteq L \subseteq \bar{K}$.

We will use the following result, which should be known from previous courses:

Theorem. For every K -homomorphism $K \hookrightarrow \bar{K}$ there exist precisely n distinct lifts $\sigma : L \rightarrow \bar{K}$.

This means $|\text{Hom}_K(L, \bar{K})| = [L : K]$. We write $\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$.

Lemma 4.14. Let $\alpha \in L$, $f = X^r + a_{r-1}X^{r-1} + \dots + a_0 \in K[X]$ the minimal polynomial of α over K and $[L : K(\alpha)] = s$. Then

1. $N_{L/K}(\alpha) = ((-1)^r a_0)^s$.

2. $\text{Tr}_{L/K}(\alpha) = -s a_{r-1}$.

Proof. We have $n = [L : K] = [L : K(\alpha)][K(\alpha) : K] = s r$ and $(1, \alpha, \dots, \alpha^{r-1})$ is a K -basis of $K(\alpha)/K$. If $\mathbf{v} = (v_1, \dots, v_s)$ is a basis of $L/K(\alpha)$, then

$$\mathbf{u} = (v_1, v_1\alpha, \dots, v_1\alpha^{r-1}; \dots; v_s, v_s\alpha, \dots, v_s\alpha^{r-1})$$

is a K -basis of L/K . We have

$$\mu_\alpha(v_i\alpha^j) = v_i\alpha^{j+1} \text{ for } j \in [0, r-2] \quad \text{and} \quad \mu_\alpha(v_i\alpha^{r-1}) = v_i(-a_0 - \dots - a_{r-1}\alpha^{r-1}).$$

So we obtain

$$A := \mathcal{M}_{\mathbf{u}, \mathbf{u}}(\mu_\alpha) = \begin{pmatrix} A_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A_1 \end{pmatrix}$$

where

$$A_1 = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{r-1} \end{pmatrix}.$$

Therefore

$$\text{Tr}_{L/K}(\alpha) = \text{Tr}(A) = s \text{Tr}(A_1) = s(-a_{r-1})$$

and

$$N_{L/K}(\alpha) = \det(A) = (\det(A_1))^s = ((-1)^{r+1}(-a_0) \cdot 1)^s = ((-1)^r a_0)^s.$$

□

Lemma 4.15. For every $\alpha \in L$ we have

$$N_{L/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) \quad \text{and} \quad \text{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

Proof. We have $K \subseteq L \subseteq \overline{K}$, $\text{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$. Let $\alpha \in L$, $f = X^r + a_{r-1}X^{r-1} + \dots + a_0 \in K[X]$ be the minimal polynomial of α over K , so that $[L : K(\alpha)] = s = n/r$. Furthermore, $f = \prod_{\nu=1}^r (X - \alpha_\nu) \in \overline{K}[X]$. Suppose w.l.o.g. $\alpha = \alpha_1$. Since L/K is separable, $\alpha, \alpha_2, \dots, \alpha_r$ are pairwise distinct. Thus there are r distinct K -monomorphism

$$\tau_\nu : K(\alpha) \rightarrow \overline{K} \text{ s.t. } \tau_\nu(\alpha) = \alpha_\nu, \text{ with } \nu \in [1, r].$$

By the theorem discussed above, since $L/K(\alpha)$ is separable, we have

$$|\{\psi : L \rightarrow \overline{K} \mid \psi \text{ is a } K\text{-homomorphism, } \psi|_{K(\alpha)} = \tau_\nu\}| = [L : K(\alpha)] = s.$$

If $\tau_{\nu,1}, \dots, \tau_{\nu,s}$ are the lifts of τ_ν , then

$$\{\sigma_1, \dots, \sigma_n\} = \{\tau_{\nu,j} \mid \nu \in [1, r], j \in [1, s]\}.$$

Therefore we obtain

$$\prod_{i=1}^n \sigma_i(\alpha) = \prod_{\nu=1}^r \prod_{j=1}^s \tau_{\nu,j}(\alpha) = \prod_{\nu=1}^r \alpha_\nu^s = \left(\prod_{\nu=1}^r \alpha_\nu \right)^s = ((-1)^r a_0)^s = N_{L/K}(\alpha)$$

and

$$\sum_{i=1}^n \sigma_i(\alpha) = \sum_{\nu=1}^r \sum_{j=1}^s \tau_{\nu,j}(\alpha) = s \sum_{\nu=1}^r \alpha_\nu = s(-a_{r-1}) = \text{Tr}_{L/K}(\alpha),$$

where the two last equalities hold by Lemma 4.14. □

Definition 4.16. If $\mathbf{u} = (u_1, \dots, u_n)$ is a basis of L/K , then

$$\Delta(\mathbf{u}) := \det \left(\text{Tr}_{L/K}(u_i u_j) \right)_{1 \leq i, j \leq n}$$

is called the *discriminant* of \mathbf{u} .

Theorem 4.17. Let $\mathbf{u} := (u_1, \dots, u_n)$ be a basis of L/K . The following hold:

1. If $\text{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$, then $\Delta(\mathbf{u}) = \det \left(\sigma_i(u_j) \right)_{1 \leq i, j \leq n}^2$.
2. If $\mathbf{v} = \mathbf{u}S$ is a basis of L/K , then $\Delta(\mathbf{v}) = \det(S)^2 \Delta(\mathbf{u})$.
3. If $L = K(\alpha)$, $\mathbf{v} := (1, \alpha, \dots, \alpha^{n-1})$ is a basis of L/K , and $\alpha, \alpha_2, \dots, \alpha_n$ are the K -conjugates of α , then $\Delta(\mathbf{v}) = \prod_{i < j} (\alpha_i - \alpha_j)^2$.
4. $\Delta(\mathbf{u}) \neq 0$. In particular, $\text{Tr}_{L/K} : L \rightarrow K$ is not the zero map.

5. There exists a basis $\mathbf{u}^* = (u_1^*, \dots, u_n^*)$ of L/K with $\text{Tr}_{L/K}(u_i u_j^*) = \delta_{i,j}$ for all $i, j \in [1, n]$. The basis \mathbf{u}^* is unique and it's called the *dual basis* of \mathbf{u} .

Proof.

1. For all $i, j \in [1, n]$, we have

$$\text{Tr}_{L/K}(u_i u_j) = \sum_{\nu=1}^n \sigma_\nu(u_i) \sigma_\nu(u_j) = \left(\sigma_1(u_i), \dots, \sigma_n(u_i) \right) \begin{pmatrix} \sigma_1(u_j) \\ \vdots \\ \sigma_n(u_j) \end{pmatrix}.$$

Thus

$$\left(\text{Tr}_{L/K}(u_i u_j) \right)_{1 \leq i, j \leq n} = A^T A,$$

where $A = \left(\sigma_i(u_j) \right)_{1 \leq i, j \leq n}$, whereby follows the assertion.

2. COPIARE.

3. COPIARE.

4. By the Primitive element Theorem, there is an $\alpha \in L$ such that $L = K(\alpha)$. Furthermore, there is an $S \in \text{GL}_n(K)$ such that $\mathbf{u} = (1, \alpha, \dots, \alpha^{n-1})S$, and hence by first point $\Delta(\mathbf{u}) = \det(S)^2 \Delta((1, \alpha, \dots, \alpha^{n-1}))$, which is trivially $\neq 0$ by point (4).

5. Since $0 \neq \Delta(\mathbf{u})$, there is a $C \in \text{GL}_n(K)$ such that

$$\left(\text{Tr}_{L/K}(u_i u_\nu) \right) \left(c_{\nu, \rho} \right) = I_n.$$

This means that for all $i, j \in [1, n]$ we have $\sum_{\nu=1}^n \text{Tr}_{L/K}(u_i u_\nu) c_{\nu, j} = \delta_{i,j}$. For all $j \in [1, n]$, define

$$u_j^* := \sum_{\nu=1}^n c_{\nu, j} u_\nu.$$

Then by linearity $\text{Tr}_{L/K}(u_i u_j^*) = \sum_{\nu=1}^n c_{\nu, j} \text{Tr}_{L/K}(u_i u_\nu) = \delta_{i,j}$. Since C is invertible, \mathbf{u}^* is a basis, and we are done (the uniqueness is immediate).

□

Corollary 4.18. Let R be integrally closed, $\mathfrak{q}(R) = K$ and L/K finite and separable.

1. If $\alpha \in L$ is integral/ R , then $N_{L/K}(\alpha) \in R$ and $\text{Tr}_{L/K}(\alpha) \in R$.

2. If $\mathbf{u} := (u_1, \dots, u_n)$ is a basis of L/K and u_1, \dots, u_n is integral/ R , then $\Delta(\mathbf{u}) \in R$.

Proof.

1. This follows from Theorem 4.7 and Lemma 4.14.
2. If, for all $i, j \in [1, n]$, u_i and u_j are integral/ R , then we already know that $u_i u_j$ is integral/ R and hence $\text{Tr}_{L/K}(u_i u_j) \in R$ by first point. This implies $\Delta(\mathbf{u}) = \det(\text{Tr}_{L/K}(u_i u_j)) \in R$.

□

4.19. Main Theorem. Let R be an integrally closed domain, $\mathbf{q}(R) = K$, L/K a finite separable field extension and $S := \text{cl}_L(R)$. The following statements hold:

1. S is an integrally closed domain, $L = \mathbf{q}(S) = \{q^{-1}\alpha \mid \alpha \in S, q \in R^\circ\}$ and $\dim(S) = \dim(R)$.
2. Let $\alpha \in L$ and $f \in K[X]$ be the minimal polynomial of α/K . Then $\alpha \in S$ iff $f \in R[X]$. In particular, $N_{L/K}[S] \subseteq R$ and $\text{Tr}_{L/K}[S] \subseteq R$.
3. Let R be noetherian. Then every ideal of S is a f.g. R -module, and S is noetherian. If R is a principal ideal domain, then every non-zero ideal of S is a free R -module of rank $[L : K]$, and every R -basis of S is a K -basis of L .

Proof.

1. $R \subseteq S$ is an integral ring extension, and hence $\dim(R) = \dim(S)$ by Cohen-Seidenberg Theorem 4.10. Let $x \in L$. Then there are $a_0, \dots, a_n \in R$ such that $a_n x^n + \dots + a_1 x + a_0 = 0$. Multiplying with a_n^{n-1} , we obtain $(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \dots + a_0 a_n^{n-1} = 0$. Then $a_n x$ is integral/ R , $a_n x \in \text{cl}_L(R) = S$, $x = a_n^{-1}(a_n x)$ and thus $L \subseteq \{q^{-1}\alpha \mid \alpha \in S, q \in R^\circ\} \subseteq \mathbf{q}(S) \subseteq L$.
2. This follows from Theorem 4.7 and Corollary 4.18.
3. Let R be noetherian and take a K -basis $\mathbf{u} = (u_1, \dots, u_n) \in L^n$ of L . By (1) we can suppose w.l.o.g. that $\mathbf{u} \in S^n$. Let $\mathbf{u}^* = (u_1^*, \dots, u_n^*)$ be its dual basis (cfr. Theorem 4.17).

Claim: $S \subseteq Ru_1^* + \dots + Ru_n^*$.

Proof: Let $\alpha \in S$ and write

$$\alpha = a_1 u_1^* + \dots + a_n u_n^*$$

for some $a_1, \dots, a_n \in K$. For $i \in [1, n]$ we obviously have $u_i \alpha \in S$ and $\text{Tr}_{L/K}(u_i \alpha) = \sum_{\nu=1}^n a_\nu \text{Tr}_{L/K}(u_i u_\nu^*) = a_i$, which is an element of R by Corollary 4.18, since $u_i \alpha \in S = \text{cl}_L(R)$. Hence $\alpha \in Ru_1^* + \dots + Ru_n^*$. ■

$Ru_1^* + \dots + Ru_n^*$ is a f.g. R -module, which by Corollary 2.36 is noetherian since R is noetherian. By the claim, S is an R -submodule of $Ru_1^* + \dots + Ru_n^*$, and thus is a noetherian R -module as well. If $\mathfrak{g} \triangleleft S$ is an ideal, then \mathfrak{g} is an S -submodule of S , and hence an R -submodule of S . Thus \mathfrak{g} is R -finitely generated. In particular, S is a noetherian domain. Now suppose R is a PID. Then

$$Ru_1 + \dots + Ru_n \subseteq S \subseteq Ru_1^* + \dots + Ru_n^*.$$

Since \mathbf{u} and \mathbf{u}^* are K -basis of L , we have that $Ru_1 + \dots + Ru_n$ and $Ru_1^* + \dots + Ru_n^*$ are free R -modules of rank n , and then the same is true for S by Theorem 2.25.

If $0 \neq \mathfrak{g} \triangleleft S$ is a nonzero ideal and $0 \neq g \in \mathfrak{g}$, then $gS \subseteq \mathfrak{g} \subseteq S$ and hence \mathfrak{g} is a free R -module of rank n by Theorem 2.53 (??? perché per forza di rango n ? a me sembra che sia perché S è free di rango n , e quindi anche gS lo è (immediato da controllare). Ma allora a cosa serve il teorema 2.53?).

If \mathbf{w} is an R -basis of S , then \mathbf{w} has n elements, and it K -generates L by first point. Hence it is a K -basis of L .

□

Lemma 4.20. Let M be a free \mathbb{Z} -module with basis $\mathbf{u} = (u_1, \dots, u_n)$ and $N \subseteq M$ a submodule with $\text{rk}(M) = \text{rk}(N)$, and with basis $\mathbf{v} = (v_1, \dots, v_n)$. Furthermore, if $A \in M_n(\mathbb{Z})$ is such that $\mathbf{v} = \mathbf{u}A$, then $0 \neq |\det(A)| = |M/N|$.

Proof. By Theorem 2.53 there are a basis $\mathbf{e} = (e_1, \dots, e_n)$ of M and $d_1, \dots, d_n \in \mathbb{Z}^\circ$ such that $(d_1 e_1, \dots, d_n e_n)$ is a basis of N . The map

$$\begin{aligned} \varphi: M &\rightarrow \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z} \\ \sum_{i=1}^n \mu_i e_i &\mapsto (\mu_1 + d_1\mathbb{Z}, \dots, \mu_n + d_n\mathbb{Z}) \end{aligned}$$

is a group epimorphism with $\ker \varphi = N$. Thus $M/N \simeq \oplus_{i=1}^n \mathbb{Z}/d_i\mathbb{Z}$, and so $|M/N| = d_1 \cdot \dots \cdot d_n$.

By hypothesis it follows immediately that there are $B, C \in \text{GL}_n(\mathbb{Z})$ such that $\mathbf{e} = \mathbf{u}C$ and $\mathbf{v} = (d_1 e_1, \dots, d_n e_n)B$. We obtain

$$\mathbf{v} = (e_1, \dots, e_n) \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & \dots & 0 & d_n \end{pmatrix} B = \mathbf{u} C \underbrace{\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & \dots & 0 & d_n \end{pmatrix}}_{=:A} B$$

and $|\det(A)| = |d_1 \cdot \dots \cdot d_n|$. Since such an A is trivially unique, we are done (??? è giusto così?). \square

Corollary 4.21. Let L/\mathbb{Q} be a finite field extension and $[L : \mathbb{Q}] = n$. Then:

1. \mathcal{O}_L is a one-dimensional integrally closed noetherian domain.
2. Every nonzero ideal $I \subseteq \mathcal{O}_L$ is a free \mathbb{Z} -module of rank n , and \mathcal{O}_L/I is finite.

Proof. \mathcal{O}_L/I is finite by Lemma 4.20. The rest of the statement follows from Theorem 4.19. \square

Remark. Let $0 \neq \mathfrak{p} \in \text{Spec}(\mathcal{O}_L)$. Then $\mathcal{O}_L/\mathfrak{p}$ is a finite domain, hence³ a field and thus $\mathfrak{p} \in \max(\mathcal{O}_L)$. This shows $\dim(\mathcal{O}_L) = 1$, without using Cohen-Seidenberg Theorem.

Definition 4.22. Let L/\mathbb{Q} be a finite field extension.

1. A \mathbb{Z} -module basis of \mathcal{O}_L is called an *integral basis of L* .
2. If \mathbf{u} is an integral basis of L , then $\Delta_L := \Delta(\mathbf{u})$ is called the *discriminant of L* .
3. If $I \triangleleft \mathcal{O}_L$ is an ideal, then $N(I) := |\mathcal{O}_L/I|$ is called the *norm of I* .

Remark. If \mathbf{u} and \mathbf{v} are integral bases of L , then there is an $S \in \text{GL}_n(\mathbb{Z})$ such that $\mathbf{v} = \mathbf{u}S$. By Theorem 4.17(2) we have

$$\Delta(\mathbf{v}) = \det(S)^2 \Delta(\mathbf{u})$$

and hence Δ_L does not depend on the choice of the integral basis.

Lemma 4.23. Let L/\mathbb{Q} be an algebraic number field, $a, b \in \mathcal{O}_L^\circ$ and $0 \neq I \triangleleft \mathcal{O}_L$. The following statements hold.

1. $N(a\mathcal{O}_L) = |N_{L/\mathbb{Q}}(a)|$.
2. $a \in \mathcal{O}_L^\times$ if and only if $|N_{L/\mathbb{Q}}(a)| = 1$.
3. If a and b are associate, then $|N_{L/\mathbb{Q}}(a)| = |N_{L/\mathbb{Q}}(b)|$.
4. If \mathbf{v} is a \mathbb{Z} -module basis of I , then $\Delta(\mathbf{v}) = N(I)^2 \Delta_L$.
5. $N(I) \in I \cap \mathbb{Z}$.

Proof.

³Recall that every finite domain is a field.

1. Let $\mathbf{u} = (u_1, \dots, u_n)$ be an integral basis of L . Then (au_1, \dots, au_n) is a \mathbb{Z} -module basis of $a\mathcal{O}_L$. If $(au_1, \dots, au_n) = (u_1, \dots, u_n)A$, then Lemma 4.20 implies $|\mathcal{O}_L/a\mathcal{O}_L| = |\det(A)|$.
On the other hand, if

$$\begin{aligned}\mu_a: L &\rightarrow L \\ u &\mapsto ua\end{aligned}$$

then

$$\begin{aligned}N_{L/\mathbb{Q}}: L &\rightarrow \mathbb{Q} \\ a &\mapsto \det(\mu_a)\end{aligned}$$

and $(\mu_a(u_1), \dots, \mu_a(u_n)) = (u_1, \dots, u_n)A$. Thus $\mathcal{M}_{\mathbf{u}, \mathbf{v}}(\mu_a) = A$, and the assertion follows.

2. We have $a \in \mathcal{O}_L^\times$ iff $a\mathcal{O}_L = \mathcal{O}_L$ iff $|\mathcal{O}_L/a\mathcal{O}_L| = 1$.
3. Since $a \sim b$ iff $a\mathcal{O}_L = b\mathcal{O}_L$, the assertion follows from (1) and (2).
4. If \mathbf{u} is an integral basis of L and $\mathbf{v} = \mathbf{u}A$, then $|\det(A)| = |\mathcal{O}_L/I|$ and hence $\Delta(\mathbf{v}) = \det(A)^2 \Delta(\mathbf{u}) = N(I)^2 \Delta(\mathbf{u})$.
5. \mathcal{O}_L/I is a finite abelian group of order $N(I) =: m$. Then $m(1+I) = m+I = 0_{\mathcal{O}_L/I}$, and thus $m \in I \cap \mathbb{Z}$.

□

Remark 4.24. *Main Results of basic Algebraic Number Theory.*

1. Ideal Theory of \mathcal{O}_L .

For a domain R , the following statements are equivalent:

- a) R is noetherian, integrally closed, and every non-zero prime ideal is maximal.
- b) Every non-zero ideal is a product of prime ideals.
- c) Every non-zero ideal is invertible.

A domain satisfying one of the equivalent conditions is called a *Dedekind domain*. By Corollary 4.21, \mathcal{O}_L is a Dedekind domain.

The following facts are easy to get:

- a) $N(IJ) = N(I)N(J)$; in particular, $N(\prod_{i=1}^g P_i^{e_i}) = \prod_{i=1}^g N(P_i^{e_i})$.
- a) If $N(I) \in \mathbb{P}$, then I is a prime ideal.

- c) For a $p \in \mathbb{P}$ and a prime ideal $0 \neq P \triangleleft \mathcal{O}_L$ there are equivalent:
- i) $P|p\mathcal{O}_L$.
 - ii) $p \in \mathbb{P}$.
 - iii) $P \cap \mathbb{Z} = p\mathbb{Z}$.
 - iv) $N(P)$ is a power of p .
- d) Let $p \in \mathbb{P}$ and $p\mathcal{O}_L = \prod_{i=1}^g P_i^{e_i}$ where $P_1, \dots, P_g \in \text{Spec}(\mathcal{O}_L)$. For $i \in [1, g]$, let $f_i = [\mathcal{O}_L/P_i : \mathbb{Z}/p\mathbb{Z}]$. Then $[L : \mathbb{Q}] = \sum_{i=1}^g e_i f_i$.

A prime p is called unramified (in L) if $e_1 = \dots = e_g = 1$, and ramified otherwise.

Theorem. p is ramified (in L) iff $p|\Delta_L$.

2. Dirichlet's Unit Theorem.

Let $\mu(L) = \{\xi \in L \mid \text{there is an } m \in \mathbb{N} \text{ s.t. } \xi^m = 1\}$ be the roots of unity of L . If $\sigma \in \text{Hom}_{\mathbb{Q}}(L, \mathbb{C})$, then $\bar{\sigma} \in \text{Hom}_{\mathbb{Q}}(L, \mathbb{C})$; σ is called real if $\sigma(L) \subseteq \mathbb{R}$ and complex otherwise. Let $\sigma_1, \dots, \sigma_r : L \rightarrow \mathbb{C}$ be the real embeddings, and

$$\sigma_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \dots, \overline{\sigma_{r+s}} : L \rightarrow \mathbb{C}$$

be the complete embeddings. Then $r + 2s = [L : \mathbb{Q}]$.

Theorem. $\mathcal{O}_L^\times \simeq \mu(L) \times \mathbb{Z}^{r+s-1}$.

3. Classgroups.

Let R be a domain, $(\mathcal{I}^*(R), \cdot)$ be the monoid of invertible ideals and $(\mathcal{H}(R), \cdot)$ the monoid of nonzero principal ideals (recall, an ideal $0 \neq I \triangleleft R$ is invertible if there is $J \triangleleft R$ s.t. $IJ \in \mathcal{H}(R)$).

We have a monoid isomorphism $R^\circ/R^\times \rightarrow \mathcal{H}(R)$, $aR^\times \mapsto aR$, and

$$K^\times/R^\times = \mathfrak{q}(R^\circ/R^\times) \simeq \mathfrak{q}(\mathcal{H}(R)) = \{aR \mid a \in K^\times\}.$$

Then $\mathcal{F}(R)^\times := \mathfrak{q}(\mathcal{I}^\times(R))$ is called the group of invertible fractional ideals,

$$\text{Pic}(R) = \mathcal{F}(R)^\times / \mathfrak{q}(\mathcal{H}(R))$$

is the Picard group of R and we have an exact sequence

$$1 \rightarrow R^\times \hookrightarrow K^\times \xrightarrow{f} \mathcal{F}(R)^\times \rightarrow \text{Pic}(R) \rightarrow 1$$

where $f(x) = xR$. If R is Dedekind, then $\mathcal{F}^\circ(R) = \mathcal{F}^*(R)$, and $\text{Pic}(R) = \text{cl}(R)$ is called the ideal class group of R .

Theorem. $\text{Pic}(\mathcal{O}_L)$ is finite.

4.4 Quadratic Number Fields.

A field extension L/K is called *quadratic* if $[L : K] = 2$. Let L/K be a quadratic field extension with $\text{char}(K) \neq 2$. Then there are $a \in L$ and $d \in K^\times \setminus K^{\times 2}$ s.t. $L = K(\alpha)$ and $\alpha^2 = d$ (we write $L(K(\sqrt{d}))$), where $K^{\times 2} = \{x^2 \mid x \in K^\times\} < (K^\times, \cdot)$. The coset $dK^{\times 2} \in K^\times/K^{\times 2}$ is uniquely determined by L .

Proof. Let $\beta \in L \setminus K$. Then $L = K(\beta)$ and $\deg_K(\beta) = 2$. Let $f = X^2 + pX + q \in K[X]$ be the minimal polynomial of β/K . Then $\beta = -p/2 + \alpha$ with $d := \alpha^2 = (p/2)^2 - q \in K$, whence $L = K(\alpha)$ and $(1, \alpha)$ is a K -basis of L . If $d = c^2$ with $c \in K$, then $f = (x + p/2 + c)(x + p/2 - c)$, which is a contradiction to the assumption f irreducible. Thus $d \in K^\times \setminus K^{\times 2}$ and it remains to show:

Claim: For $i \in [1, 2]$, let L_i/K be a quadratic extension with $L_i = K(\alpha_i)$ and $\alpha_i^2 = d_i \in K$. Then $L_1 = L_2$ iff $d_1 K^{\times 2} = d_2 K^{\times 2}$.

Proof: (\Rightarrow) Since $L_1 = L_2$, there are $a, b \in K$ with $\alpha_1 = a + b\alpha_2$, and hence $d_1 = a^2 + 2ab\alpha_2 + b^2\alpha_2^2 \in K$. Since $(1, \alpha_2)$ is a K -basis, it follows that $ab = 0$ and since $\alpha_1 \notin K$ we get $b \neq 0$. Thus $a = 0$ and we have $d_1 = b^2 d_2$, and therefore $d_1 K^{\times 2} = d_2 K^{\times 2}$.

(\Leftarrow) Since $d_1 K^{\times 2} = d_2 K^{\times 2}$, we obtain $d_1 = b^2 d_2$ with $b \in K^\times$, whence $\alpha_1 = \pm b\alpha_2$ and thus $L_2 = K(\alpha_2) = K(\alpha_1) = L_1$. ■

□

Definition 4.25. An algebraic number field K/\mathbb{Q} is called *quadratic* if $[K : \mathbb{Q}] = 2$. For $d \in \mathbb{Z}$ we set

$$\sqrt{d} = \begin{cases} \text{positive real root in } \mathbb{R}_{\geq 0} & \text{if } d > 0 \\ i\sqrt{|d|} \in i\mathbb{R}_{>0} & \text{if } d < 0 \end{cases}$$

Theorem 4.26. Let K be a quadratic number field.

1. (i) There is precisely one squarefree $d \in \mathbb{Z} \setminus \{0, 1\}$ with $K = \mathbb{Q}(\sqrt{d})$, $X^2 - d \in \mathbb{Q}[X]$ is the minimal polynomial of \sqrt{d} , and $(1, \sqrt{d})$ is a \mathbb{Q} -basis of K .
(ii) K/\mathbb{Q} is Galois and $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \sigma_2\}$, with $\sigma_1, \sigma_2 : K \rightarrow \mathbb{C}$, $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$, $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$.
(iii) For all $a, b \in \mathbb{Q}$, we have $N_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - b^2 d$ and $\text{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a$.
2. (i) If $d \equiv 2, 3 \pmod{4}$, then $(1, \sqrt{d})$ is an integral basis of K , $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, and $\Delta_K = 4d$.
(ii) If $d \equiv 1 \pmod{4}$, then $(1, \frac{1+\sqrt{d}}{2})$ is an integral basis of K , $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, and $\Delta_K = d$.

Proof.

1. Suppose $a = \varepsilon \prod_{p \in \mathbb{P}} p^{V_p(a)} \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$ with $\varepsilon \in \{-1, 1\}$. Since K is uniquely determined by

$$a\mathbb{Q}^{\times 2} = \varepsilon \prod_{V_p(a) \equiv 1 \pmod{2}} p\mathbb{Q}^{\times 2} \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2} \quad (*)$$

and since $\prod_{V_p(a) \equiv 1 \pmod{2}} p$ is the only squarefree $d \in \mathbb{Z} \setminus \{0, 1\}$ satisfying relation $(*)$, the uniqueness of d in 1.(ii) follows, and 1.(iii) follows from Lemma 4.15.

2. \sqrt{d} is a zero of $X^2 - d$, and hence $\sqrt{d} \in \mathcal{O}_K$. If $d \equiv 1 \pmod{4}$, then $f = X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X]$ monic, $f(\frac{1+\sqrt{d}}{2}) = 0$, and hence $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$. The tuples $(1, \sqrt{d}), (1, \frac{1+\sqrt{d}}{2})$ are \mathbb{Q} -linear independent, and hence \mathbb{Z} -linear independent. Thus it remains to show that $\mathcal{O}_K \subseteq \mathbb{Z}\langle 1, \sqrt{d} \rangle$ resp. $\mathcal{O}_K \subseteq \mathbb{Z}\langle 1, (1 + \sqrt{d})/2 \rangle$. Let $\alpha \in \mathcal{O}_K$. Then there are $a, b \in \mathbb{Q}$ s.t. $\alpha = a + b\sqrt{d}$ and Cor.4.18 implies $N_{K/\mathbb{Q}}(\alpha) = a^2 - b^2d$ and $\text{Tr}_{K/\mathbb{Q}}(\alpha) = 2a \in \mathbb{Z}$.

Then

$$4(a^2 - b^2d) - (2a)^2 = (2b)^2d \in \mathbb{Z}$$

and since d is squarefree, we obtain $2b \in \mathbb{Z}$. We set $a' = 2a, b' = 2b$, whence $\alpha = \frac{a'}{2} + \frac{b'}{2}\sqrt{d}$ and $a'^2 - b'^2d \equiv 0 \pmod{4}$.

Case 1. $d \equiv 2, 3 \pmod{4}$. Then $a'^2 \equiv 2b'^2 \pmod{4}$ or $a'^2 \equiv 3b'^2 \pmod{4}$. This implies that $a' \equiv b' \equiv 0 \pmod{2}$ and hence $\alpha \in \mathbb{Z}\langle 1, \sqrt{d} \rangle$.

Case 2. $d \equiv 1 \pmod{4}$. Then $a'^2 \equiv b'^2 \pmod{4}$ and hence $a' \equiv b' \pmod{2}$. Therefore

$$\alpha = \frac{a'}{2} + \frac{b'}{2}\sqrt{d} = \frac{a' - b'}{2} + b' \frac{1 + \sqrt{d}}{2} \in \mathbb{Z} \left\langle 1, \frac{1 + \sqrt{d}}{2} \right\rangle.$$

On the discriminant.

Case 1. $d \equiv 2, 3 \pmod{4}$.

$$\Delta_K = \Delta\left((1, \sqrt{d})\right) \stackrel{4.17.1}{=} \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d.$$

Case 2. $d \equiv 1 \pmod{4}$.

$$\Delta_K = \Delta\left(\left(1, \frac{1 + \sqrt{d}}{2}\right)\right) = \det \begin{pmatrix} 1 & \frac{1 + \sqrt{d}}{2} \\ 1 & \frac{1 - \sqrt{d}}{2} \end{pmatrix}^2 = \left(\frac{1 + \sqrt{d}}{2} - \frac{1 - \sqrt{d}}{2}\right)^2 = d.$$

□

Definition 4.27. Let $m, n \in \mathbb{N}_{\geq 2}$. An integer $a \in \mathbb{Z}$ is called n -th power residue modulo m if there is an $x \in \mathbb{Z}$ such that $x^n \equiv a \pmod{m}$ (equivalently, if $(a + m\mathbb{Z})$ is n -th power in $\mathbb{Z}/m\mathbb{Z}$). For $n = 2$ ($n = 3, n = 4$) these are called *quadratic* (*cubic*, *biquadratic*) residues modulo m .

Theorem 4.28. Let $K := \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z} \setminus \{0, 1\}$ squarefree a quadratic number field with discriminant Δ_K , integer ring $R := \mathcal{O}_K$. Let $p \in P$.

1. If $p | \Delta_K$, then

$$pR = \begin{cases} \langle 2, 1 + \sqrt{d} \rangle^2, & \text{if } p = 2 \text{ and } d \equiv 3 \pmod{4}, \\ \langle p, \sqrt{d} \rangle^2, & \text{otherwise.} \end{cases}$$

2. Let p be odd and $p \nmid \Delta_K$. If d is quadratic residue modulo p , then $pR \in \text{Spec}(R)$. If $d \equiv n^2 \pmod{p}$, then $pR = \langle p, n + \sqrt{d} \rangle \langle p, n - \sqrt{d} \rangle$.
3. Let $2 \nmid \Delta_K$ (then $d \equiv 1 \pmod{4}$). If $d \equiv 5 \pmod{8}$, then $2R \in \text{Spec}(R)$. If $d \equiv 1 \pmod{8}$, then $2R = \langle 2, \frac{1+\sqrt{d}}{2} \rangle \langle 2, \frac{1-\sqrt{d}}{2} \rangle$.

Proof.

1. Let $p | \Delta_K$. We check that $pR = P^2$ and P as above. From $\sum_{i=1}^g e_i f_i = 2$ follows that $P \in \text{Spec}(R)$.

CASE 1: $p \equiv 1 \pmod{2}$ and $p | \Delta_K$. Then $p | d$. We have that $\langle p, \sqrt{d} \rangle^2 = \langle p^2, p\sqrt{d}, d \rangle = pR$.

\subseteq Immediate since it is a multiple of p .

\supseteq From d squarefree follows that $\gcd(p, \frac{d}{p}) = 1$. Then there are $x, y \in \mathbb{Z}$ such that $px + \frac{d}{p}y = 1$ and $p = p^2x + dy \in \langle p^2, p\sqrt{d}, d \rangle$.

CASE 2: $p = 2, d \equiv 1, 2 \pmod{4}, p | \Delta_K$. Then $2 | d$. We have $\langle 2, \sqrt{d} \rangle^2 = \langle 4, 2\sqrt{d}, d \rangle = 2R$.

\subseteq Immediate.

\supseteq As above $\gcd(2, \frac{d}{2}) = 1$ and thus $2 = 4x + dy$.

CASE 3: $p = 2$ and $d \equiv 3 \pmod{4}$. Then $\langle 2, 1 + \sqrt{d} \rangle^2 = \langle 4, 2 + 2\sqrt{d}, 1 + d + 2\sqrt{d} \rangle 2R$.

\subseteq Immediate.

\supseteq Because $d - 1 \in \langle \dots \rangle$, and thus

$$2 = (d - 1) + 4x \in \langle 4, 2 + 2\sqrt{d}, 1 + d + 2\sqrt{d} \rangle.$$

2. Let p be odd and $p \nmid \Delta_K$.

CASE 1: Let $d \equiv n^2 \pmod{p}$. We check that $pR = P_1P_2$ with P_1P_2 as before. Then $P_1, P_2 \in \text{Spec}(R)$. We have

$$\langle p, n + \sqrt{d} \rangle \langle p, n - \sqrt{d} \rangle = \langle p^2, pn + p\sqrt{d}, pn - p\sqrt{d}, n^2 - d \rangle = pR.$$

\subseteq Immediate.

\supseteq From $p \nmid 2n$ follows that there are $x, y \in \mathbb{Z}$ with $1 = 2nx + py$ and thus

$$p = (2np)x + p^2y \in \langle p^2, pn + p\sqrt{d}, pn - p\sqrt{d}, n^2 - d \rangle.$$

CASE 2: The congruence $x^2 \equiv d \pmod{p}$ has no solutions. By Cohen-Seidenberg Theorem, there is a $P \in \text{Spec}(R)$ such that $P \cap \mathbb{Z} = p\mathbb{Z}$, and we claim that $P = pR$.

The polynomial $f := X^2 - d$ has no root in $\mathbb{Z}/p\mathbb{Z}$, but the polynomial $X^2 - d$ has a root in R and thus in R/P . By this follows $\mathbb{Z}/p\mathbb{Z} \not\cong R/P$, thus $N(P) = |R/P| = p^2$, and $pR = P \in \text{Spec}(R)$ from $g = 1$ and $p_1 = 2$.

3. CASE 1: $d \equiv 1 \pmod{8}$. We have

$$\left\langle 2, \frac{1 + \sqrt{d}}{2} \right\rangle \left\langle 2, \frac{1 - \sqrt{d}}{2} \right\rangle = \left\langle 1, 1 + \sqrt{d}, 1 - \sqrt{d}, \frac{1 - d}{4} \right\rangle = 2R.$$

\subseteq Immediate.

\supseteq We have $2 = (1 + \sqrt{d}) + (1 - \sqrt{d}) \in \langle 1, 1 + \sqrt{d}, 1 - \sqrt{d}, \frac{1-d}{4} \rangle$.

CASE 2: $d \equiv 5 \pmod{8}$. By Cohen-Seidenberg, there is a $P \in \text{Spec}(R)$ with $P \cap \mathbb{Z} = 2\mathbb{Z}$. $f := X^2 - X + \frac{1-d}{4}$ has root in R and thus in R/P . $\bar{f} := X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ has no roots in $\mathbb{Z}/2\mathbb{Z}$. Thus $R/P \not\cong \mathbb{Z}/2\mathbb{Z}$ and thus $P = 2R \in \text{Spec}(R)$.

□

Lemma 4.29 (Pell's equation). For every square-free $d > 0$, Pell's equation $X^2 - dY^2 = 1$ has infinitely many integer solutions. Such solutions are (??? precisely?) of the form

$$\pm(x_n, y_n) \text{ with } x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \text{ and } n \in \mathbb{Z}. \text{ (??? cos'è } (x_1, y_1)\text{?)}$$

Theorem 4.30 (Units in integer rings of quadratic number fields). Let $K := \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z} \setminus \{0, 1\}$ square-free be a quadratic number field, and $R := \mathcal{O}_K$ its integer ring.

1. If $d < 0$, then $R^\times = \mu(K)$ and

$$\mu(K) = \begin{cases} \{-1, 1, i, -i\}, & \text{if } d = -1 \\ \left\langle \frac{1-\sqrt{-3}}{2} (= -e^{\frac{2\pi i}{3}}) \right\rangle, & \text{if } d = -3 \\ \{-1, 1\}, & \text{otherwise} \end{cases}$$

2. If $d > 0$, then there is a unit $\varepsilon > 1$ such that every unit is of the form $\pm \varepsilon^m$ for some $m \in \mathbb{Z}$. Then

$$\mu(K) = \{-1, 1\} \text{ and } R^\times = \mu(K) \times \langle \varepsilon \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Proof.

1. Let $d \equiv 2, 3 \pmod{4}$. If $\varepsilon \in R^\times$, then there are $x, y \in \mathbb{Z}$ with $\varepsilon = x + y\sqrt{d}$, and $|N_{K/\mathbb{Q}}(\varepsilon)| = x^2 - dy^2 = 1$. If $d = -1$, then $x, y \in \{-1, 1\}$. If $-d > 1$, then $y = 0$ and $\varepsilon \in \{-1, 1\}$. Let $d \equiv 1 \pmod{4}$, and $\varepsilon \in R^\times$. Then there are $x, x', y \in \mathbb{Z}$ such that

$$\varepsilon = x' + y \frac{1 + \sqrt{d}}{2} = \frac{2x' + y + y\sqrt{d}}{2} = \frac{x + y\sqrt{d}}{2},$$

with $x \equiv y \pmod{2}$. From $|N_{K/\mathbb{Q}}(\varepsilon)| = 1$ follows $x^2 + dy^2 = 4$.

If $d = -3$, then the statement follows. If $|d| > 3$, then $y = 0$ and $\varepsilon \in \{-1, 1\}$.

2. Let $d > 0$. By Lemma 4.29 there are $x, y \in \mathbb{N}$ s.t. $x^2 - dy^2 = 1$. Thus $u = x + y\sqrt{d} \in R^\times$ and $u > 1$. Let $M \in \mathbb{R}_{\geq 0}$ with $u < M$. Then there are only finitely many $\alpha \in R$ such that

$$|\alpha = \sigma_1(\alpha)| < M \text{ and } |\sigma_2(\alpha)| < M.$$

If $\beta \in R^\times$ with $1 < \beta < M$ and $\beta' = \sigma_2(\beta)$, then $N_{K/\mathbb{Q}}(\beta) = \beta\beta' \in \{-1, 1\}$. If $\beta' = \frac{-1}{\beta}$, then $-M < -\frac{1}{\beta} < M$, and if $\beta' = \frac{1}{\beta}$, then $-M < \frac{1}{\beta} < M$. Thus there are only finitely many $\beta \in R^\times$ such that $1 < \beta < M$ and u has this property. Let $\varepsilon > 1$ the smallest unit with this property. Let $\tau \in R^\times$ be s.t. $\tau > 0$. Then there is an $s \in \mathbb{Z}$ with $\varepsilon^s \leq \tau \leq \varepsilon^{s+1}$. Thus it follows that $1 \leq \tau\varepsilon^{-s} < \varepsilon$, and from $\tau\varepsilon^{-s} \in R^\times$ follows that $\tau\varepsilon^{-2} = 1$. If $\tau < 0$ then $-\tau > 0$ and $-\tau = \varepsilon^s$.

□

Bibliography

- [1] James W. Brewer, Sarah Glaz, William Heinzer, Bruce Olberding, *Multiplicative Ideal Theory in Commutative Algebra: A Tribute to the Work of Robert Gilmer*. Springer Science & Business Media, Dec 15, 2006.