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

- $R = \{0\} \Longleftrightarrow 0 = 1$.

- $0 \in \mathrm{Zdv}(R) \Longleftrightarrow R \neq \{0\}$.

- $R^\times \cap \mathrm{Zdv}(R) = \emptyset$ (if $a \in R^\times$ and $x \in R$, 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 $\mathrm{Zdv}(R) = \{0\}$ ($\Longleftrightarrow R^\circ$ is multiplicatively closed $\Longleftrightarrow R^\circ \subseteq R$ 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 $\mathsf{q}(R)$ and that every finite domain is a field.

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

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 $p \notin H^\times$ 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: $\mathbb{N} = \{1, 2, ...\}$ and $\mathbb{N}_0 = \{0, 1, 2, ...\}$.)

- $M = (N, \cdot)$

- $M(4\,\mathbb{N}_0 + 1, \cdot)$. 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. $\forall a \in M \setminus M^\times \exists l \in \mathbb{N} \exists u_1, ..., u_l \in \mathcal{A}(M)$ s.t. $a = u_1 \cdot ... \cdot u_l$). Observe that the 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 $(R^\circ, \cdot)$ is atomic (resp. factorial).

Examples.

1. Fundamental Theorem of Arithmetic: $(\mathbb{N}, \cdot)$ is factorial (and $\mathbb{Z}$ is factorial).

2. Every Euclidean domain[1] is factorial. The polynomial ring over a field in one indeterminate is Euclidean with $\delta := \deg$.

3. $M = (\mathbb{N}_0 + 1, \cdot)$ 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 $a \in A$.
   (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.

---

[1]Recall the definition of *Euclidean domain*: a ring R is an Euclidean domain if there exists a map $\delta : R^\circ \to \mathbb{N}_0$ 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.

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 representatives[2] 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 $\{2, 3, 5, 7, ...\}$. Of course also $\{2, -3, -5, 7, 11, -13, ...\}$ 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. No proof. (???)

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 $c'|c$. We can assume WLOG that b' is a unit (??? perché? devo stare attento alla condizione $c'|c$!!!), whereby $p|c$.

$\square$

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

---

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

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

1. Let $m, n \in \mathbb{N}_0$ and let $p_1, ..., p_n, q_1, ..., q_m \in M$ 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 $p_1 \cdot ... \cdot p_n \cdot c \simeq q_1 \cdot ... \cdot q_m \cdot d$. 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 $a = p_1 \cdot ... \cdot p_n \cdot c$, with $n \in \mathbb{N}$, $p_1, ..., p_n \in P$ and $c \in M$, where c is not divisible by any $p \in P$. Furthermore, $p_1, ..., p_n$ and c are uniquely determined (up to the order and up to associates).

3. Let M be atomic, $p \in M$ prime, and $a \in \mathsf{q}(M)$. 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 $p_1 | q_1 \cdot ... \cdot q_m d$, and since $p_1 \nmid d$ we obtain by primality that $p_1 | q_j$ for some $j \in [1, m]$. Since $p_1, q_j \in \mathcal{A}(M)$, we get $p_1 \simeq q_j$ and hence
$$p_2 \cdot ... \cdot p_n \cdot c \simeq q_1 \cdot ... \cdot q_{j-1} \cdot q_{j+1} \cdot ... \cdot q_m \cdot d.$$
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 $a = \varepsilon \cdot r_1 \cdot ... \cdot r_n$, where $n \in \mathbb{N}_0$ and $r_1, ..., r_n \in \mathcal{A}(M)$. After renumbering if necessary, there is an $m \in [0, n]$ s.t. $r_j \in P$ (???NOTA: mi sa che bisogna aumentare un po' la generalità...ovvero, "s.t. $r_j \simeq p$ for some $p \in P$") for each $j \in [1, m]$ and $r_j \not\simeq p$ for any $p \in P$, $j \in [m+1, n]$. Thus the assertion holds with $c = \varepsilon \cdot r_{m+1} \cdot ... \cdot r_n$.

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 $a \in \mathsf{q}(M)$, then $a = a_0^{-1} a_1$ for some $a_0, a_1 \in M$. For $i \in \{0, 1\}$, we can write $a_i = p^{n_i} b$ 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
$$v p^n \frac{b}{c} = va = a_1 = (up)^{n_1} \frac{b_1}{c_1},$$

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. $n = n_1$. $\qquad\square$

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

Definition 1.4. The map $v_p : \mathsf{q}(M) \to \mathbb{Z}$ 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 associate 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

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

(??? does A have to be finite here? otherwise, this also means that if M is factorial then the gcd is never empty (which is not a problem, of course))

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

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

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

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

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. $\qquad\square$

1.2 Rings and Ideals

Let R be a ring and $I, J \lhd R$ 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 $\theta : R^\circ \setminus R^\times \to \mathcal{H}(R)$ given by $aR^\times \mapsto aR$ is a semigroup isomorphism. The group $K^\times / R^\times := \mathsf{q}(R^\circ/R^\times) \simeq \mathsf{q}(\mathcal{H}(R)) = \{aR \mid a \in K^\times\}$ is called *group of divisibility*.

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

(a) R/I is a domain.

(b) If $a, b \in R$ and $ab \in I$, then $a \in I$ or $b \in I$.

(c) If $A, B \lhd R$ and $AB \subseteq I$, then $A \subseteq I$ or $B \subseteq I$.

(d) $R \setminus I$ is multiplicatively closed.

Proof.
(a)$\Leftrightarrow$(b): Well known[3]
(b)$\Leftrightarrow$(d): Trivial by definition.
(c)$\Rightarrow$(b): It's sufficient to consider singletons.
(b)$\Rightarrow$(c): By contraposition. Suppose $AB \subseteq I$, $A \nsubseteq I$ and $B \nsubseteq I$. Then there are $a \in A \setminus I$, $b \in B \setminus I$ and $ab \in AB \subseteq I$, i.e. $\neg$(b). $\qquad\square$

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. $I \nsubseteq J \nsubseteq R$.

It is a well-know result that an ideal $I \lhd R$ is maximal if and only if R/I is a field[4].
The following results should be already known by the reader.

---

[3]See   `https://proofwiki.org/wiki/Prime_Ideal_iff_Quotient_Ring_is_Integral_Domain`.

[4]See `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 $pR \lhd R$ 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 $\mathrm{Spec}(R)$ the set of prime ideals, and by $\max(R)$ the set of maximal ideals.

5. Let R be a domain. Then R is factorial $\overset{\text{def}}{\Leftrightarrow} (R^\circ, \cdot)$ is factorial $\Leftrightarrow (\mathcal{H}(R), \cdot)$ is factorial.

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

1. $\{pR \mid p \in R \text{ is prime}\} = \mathrm{Spec}(R) \setminus \{(0)\}$.

2. $\mathrm{Spec}(R) \setminus \{(0)\} = \max(R)$.

3. $\mathcal{F}^\circ(R) = \mathcal{H}(R)$, it is factorial and $\mathrm{Spec}(R) \setminus \{(0)\}$ 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 $I = bR \lhd R$ such that $pR \nsubseteq bR \lhd R$. 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 $p \mid c$, 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.

$\square$

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 ($\langle X \rangle \nsubseteq \langle X, Y^2 \rangle \nsubseteq K[X, Y]$).
   - $R = \mathbb{Z}[X]$ 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 $\mathrm{Spec}(R) \setminus \{(0)\}$ 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

$$R \times M \to M$$
$$(\lambda, x) \mapsto \lambda \cdot x = \lambda x$$

such that for all $\lambda, \mu \in R$ and all $x, y \in M$ the follwing 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 multiplication as scalar multiplication).

4. The ring multiplication $R \times R \to R$, $(x, y) \mapsto x \cdot_R y$ is an R-module structure, i.e. R is an R-module.

5. Let $f : R \to S$ be a ring homomorphism. Then S is an R-module with the structure

$$R \times S \to S$$
$$(r, s) \mapsto f(r)s.$$

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

Definition 2.2. Let M be an R-module. A subset $N \subseteq M$ is called an *(R-)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 $\cdot_{|_{R \times N}}; R \times N \to N$ 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 $\{0_R\}$. 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

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

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

$$_R\langle E\rangle := \langle E\rangle := \left\{ \sum_{i=1}^{n} \;\middle|\; n \in \mathbb{N}, \; \lambda_1, \dots, \lambda_n \in R, \; x_1, \dots, x_n \in E \right\}$$

is the *submodule generated by E*.

Remark.

1. It is immediate to check that

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

   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 $\langle \cup_{j\in J} M_j\rangle = \sum_{j\in J} M_j$.

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 $M = \langle E\rangle \subseteq \langle\langle E''\rangle\rangle = \langle E''\rangle$. $\qquad\square$

Definition 2.4. Let M and N be R-modules. A map $f : M \to N$ 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 $\mathrm{Hom}_R(M, N)$ as the set of all R-homomorphisms $M \to N$ and $\mathrm{End}_R(M) :=$ $\mathrm{Hom}_R(M, M)$, 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. We have:

   (a) $f[M'] \subseteq N$ and $f^{-1}[N'] \subseteq M$ are R-submodules. In particular $\mathrm{Im}(f) :=$ $f[M] \subseteq M$ and $\ker(f) := f^{-1}(0) \subseteq M$ are R-submodules.

   (b) If $f[M'] \subseteq N'$, then $f_{|_{M'}} : M' \to N'$ is an R-homomorphism. In particular, $f : M \to f[M]$ is an R-epimorphism.

3. Let $g : M \to N$ be an R-homomorphism and $E \subseteq M$. We have:

   (a) $\langle f[E] \rangle = f[\langle E \rangle]$.

   (b) $f_{|_E} = g_{|_E} \Leftrightarrow f_{|_{\langle E \rangle}} = g_{|_{\langle E \rangle}}$.

   oblique

4. If $f : M \to N$ and $g : N \to P$ 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 $f, g \in \mathrm{Hom}_R(M, N)$, then $f + g$ and $-f$ are R-homomorphisms $M \to N$, where the function are define as pointwise sum and inverse. Now observe that

$$\alpha f : M \to N$$
$$x \mapsto \alpha f(x)$$

   is a group homomorphism. Finally, $\lambda(\alpha f) = (\lambda \alpha) f$.
   We have just proved the following: $\mathrm{Hom}_R(M, N)$ is an R-module w.r.t. pointiwise addition and scalar multiplication $(\alpha, f) \mapsto \alpha f$.

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

2.1.2 Congruence relation 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*

$$\pi_\sim = \pi : M \to M/\sim$$
$$a \mapsto [a].$$

2. Suppose that $* : M$ is a binary operation on M, i.e. $* : M \times M \to M$. 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 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 $\pi : M \to M/\sim$ 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! $\qquad\square$

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 $\sim \ = \ \equiv_\sim$.

   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 $\sim \ = \ \equiv_\sim$. $\qquad\square$

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

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 $\pi_M \to M/N$ is an R-epimorphism. We have that the structure is

$$\cdot : R \times M/N \to M/N$$
$$(\lambda, [a]) \mapsto [\lambda a].$$

Proof. Exercise. $\qquad\square$

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

$$\{N' \subseteq M \mid N \subseteq N' \subseteq M, \ N' \ R\text{-subm.}\} \to \{R\text{-submodules of } M/N\}$$
$$N' \mapsto N'/N = \pi[N']$$
$$\pi^{-1}[P] \mapsfrom P$$

are bijections which are inverse to each other. (??? perché è un corollario?)

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

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

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 $f^* : M/\sim_f \to f[M]$ and a unique injection $\overline{f} : M/\sim_f \to \overline{M}$ such that the following diagram commutes:

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

i.e. $\overline{f}([a]_{\sim_f}) = f(a)$ and $f^*([a]_{\sim_f}) = f(a)$. (??? chiedere se così il diagramma è giusto).

Lemma 2.11 (Abstract homomorphism theorem). Let $f : (M, *) \to (M, \cdot)$ be a semigroup homomorphism. Then $\sim_f$ is a congruence relation on M, and $f^* : M/\sim_f \to f[M]$ is a $(\tilde{*}, \cdot)$ homomorphism which is bijective, where $M/\sim_f$ is equipped with $\tilde{*}$. i.e. the operation induced by $*$ (see Lemma 2.6). (??? chiedere se era effettivamente questo che si intendeva)

Theorem 2.12 (Homomorphism Theorem for Modules)**.** Let $f : M \to N$ 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 $f^* : M/M' \to N/N'$ satisfying

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

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

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

Moreover, $\ker(f^*) = f^{-1}[N']/M'$ and $\operatorname{Im}(f^*) = (f[M] + N')/N'$.
As a special case, suppose $M' = \ker(f)$ and $N' = 0$. Then $f^* : M/\ker(f) \to N$ is an R-monomorphism[1] 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 funciton 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

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

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 $\operatorname{Im}(f^*)$ have the given form. $\qquad\square$

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

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

is an isomorphism.

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

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

---

[1] Of course, we identify N and $N/0$.

with

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

and

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

$\square$

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

$$\tilde{f} \colon (M/B)/(A/B) \to M/A$$
$$(a + B) + (A/B) \mapsto a + A$$

is an isomorphism.

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

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 $\mathrm{Zdv}_R(M)$ as the set of zero-divisors on M.
   M is called *R-torsionfree* if $\mathrm{Zdv}_R(M) = 0$.

2. Let $E \subseteq M$ be a subset. Then

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

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

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

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

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

17

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 $\mathfrak{g} \lhd R$ such that $M \simeq R/\mathfrak{g}$.

Proof.
"$\Rightarrow$": If $M = Rx$ with $x \in M$, then $f : R \to M$ given by $\lambda \mapsto \lambda x$ is an R-epimorphism with $\ker f = \operatorname{Ann}_R(M) \lhd R$.
"$\Leftarrow$": Since $\pi : R \to R/\mathfrak{g}$ is an R-epimorphism and $R = {}_R\langle 1 \rangle$, $R/\mathfrak{g}$ is cyclic by point (3) of the remark above. $\qquad\square$

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

$$\varphi \colon M \to \operatorname{Hom}_R(R, M)$$
$$x \mapsto (\lambda \mapsto \lambda x)$$

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

   $$\psi \colon \operatorname{Hom}_R(R, M) \to M$$
   $$g \mapsto g(1).$$

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

18

$\square$

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

1. The function

$$R/I \times M \to M$$
$$(\lambda + I, m) \mapsto \lambda m$$

   is an R/I-module structure on M.

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

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

   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 $\lambda - \lambda' \subseteq \mathrm{Ann}_R(M)$, and thus for all $x \in M$ we get $(\lambda - \lambda')x = 0$, i.e. $\lambda x = \lambda' x$.

2. "$\subseteq$": Let $f \in \mathrm{Hom}_R(M, N)$. 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 $f \in \mathrm{Hom}_{R/I}(M, N)$. We have to verify that f is R-linear. If $\lambda \in R$ and $x \in M$, then

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

$\square$

Examples. Observe that for $R = \mathbb{Z}$, $I = p\mathbb{Z}$, $N = \mathbb{Z}/p\mathbb{Z}$, Theorem 2.18 implies that the group 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 $I \lhd R$ an ideal. Then

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

Remark.

1. $IM \subseteq M$ is an R-submodule.

2. If $M = J \lhd R$ then IJ is the usual ideal multiplication.

3. If $J \lhd R$, then $(IJ)M = I(JM)$.

4. Since $I \subseteq \mathrm{Ann}_R(M/IM)$, M/IM carries an R/I-module structure by the previous results.

2.1.3 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

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

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

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

$$p_j \colon \prod_{i \in I} M_i \to M_j \qquad \text{and} \qquad \varepsilon_j \colon M_j \to \prod_{i \in I} M_i$$
$$(x_i)_{i \in I} \mapsto x_j \qquad\qquad\qquad x_j \mapsto (..., 0, x_j, 0, ...)$$

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 $i \in I$, the 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

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

   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

$$g \colon \bigoplus_{i \in I} M_i \to M$$

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

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

(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 $j \in I$, $M \cap \sum_{i \in I \setminus \{j\}} = 0$.

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

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

   are isomorphisms.

Proof. Let $g : \bigoplus_{i \in I} M_i \to M$ 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 $j \in J$. Thus $x_j \in M \cap \sum_{i \in I \setminus \{j\}}$ for all $j \in J$, 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).

$\square$

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

$$g \colon R^{(I)} \to M$$
$$(\lambda_i)_{i \in I} \mapsto \sum_{i \in I} \lambda_i e_i.$$

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

- *(R-)linearly independent* if g is an R-monomorphism.

- an *(R-)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:

  $(e_i)_{i \in I}$ 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 $a \notin \mathrm{Zdv}(R)$.
   - 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 $K := \mathsf{q}(R)$. 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 $\mathrm{Ann}_R(e_i) = 0$ for all $i \in I$.

3. If M is free, then $\mathrm{Zdv}_R(M) \subseteq \mathrm{Zdv}_R(R)$. In particular, if R is a domain then every free module is torsionfree.

4. If M is free, then $\mathrm{Ann}_R(M) = 0$.

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

Proof.

1. "$\Rightarrow$": M is free, i.e. by definition there exists an R-isomorphism $f : R^{(I)} \to M$. 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.
   "$\Leftarrow$": Observe that by hypothesis it immediately follows that

$$g : R^{(I)} \to M$$
$$(\lambda_i)_{i \in I} \mapsto \sum_{i \in I} \lambda_i e_i$$

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

2. Consider

$$g: \quad R^{(I)} \overset{\varphi}{\to} \bigoplus_{i \in I} Re_i \overset{\psi}{\to} M$$

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

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

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

3. Let $(e_i)_{i \in I}$ be a basis of M and $c \in \mathrm{Zdv}_R(M)$. 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. $c \in \mathrm{Zdv}_R(R)$.

4. If $(e_i)_{i \in I}$ is a basis of M, then $\mathrm{Ann}_R(M) \subseteq \mathrm{Ann}_R(e_i) = 0$ 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

$$f: M \to N$$

$$x \mapsto \sum_{b \in B} \lambda_b f_\circ(b)$$

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

$\square$

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 $\mathrm{Ann}_R(R/aR) = aR \neq 0$. 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 $z \in M \setminus \langle B^* \rangle$.

<u>Claim:</u> $B^* \cup \{z\}$ is linearly independent.

<u>Proof:</u> 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. $\blacksquare$

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.

<u>Claim:</u> $\mathrm{Zdv}(R) = \{0\}$, i.e. R is a domain.

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

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

"$\Rightarrow$": 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 $f : C' \to {}_R\langle C \rangle \cap N$ is 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 way[4]

$$(C, C', f) \leq (D, D', g) \Leftrightarrow (C \subseteq D, C' \subseteq D', f \subseteq g).$$

By considering the union of chains as usual, it is immediate to check that $(\Omega, \leq)$ 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

---

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

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

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

to the contrary that there is a $u \in B \setminus C$. Define $D := C \cup \{u\}$ and observe that

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

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 $(D, C', f) \gneqq (C, C', f)$, which contradicts the maximality of (C, C', f).
CASE 2: $\langle D \rangle \cap N \supsetneqq \langle C \rangle \cap N$. 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 $0 \neq \mathfrak{a} \lhd R$, 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

$$g : D' \to \langle D \rangle \cap N$$
$$g_{|C'} := f$$
$$u \mapsto x + au.$$

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

<u>Proof:</u> We proceed in two steps:

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

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 is 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 $(D, D', g) \gneqq (C, C', f)$, which contradicts the maximality of (C, C', f).

□

Chapter 3

Ideal Theory

In this section, let R be a ring.

3.1 Prime ideals and maximal ideals

3.1. Krull's Existence Theorem. Let $I \lhd R$ be an ideal, $T \subseteq R$ a multiplicatively closed subset of R with $T \cap I = \emptyset$ and let $\Omega = \{J \lhd R \mid I \subseteq J, J \cap T = \emptyset\}$. 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 $p_1 + c_1 a \in T$ and $p_2 + c_2 b \in T$. Then

$$(p_1 + c_1 a)(p_2 + c_2 b) = (p_2 + c_2 b)p_1 + (c_1 a)p_2 + (c_1 c_2)ab \in P \cap T = \emptyset,$$

contradiction.

$\square$

Corollary 3.2. Let $R \neq 0$.

1. Every proper ideal $I \lhd R$ is contained by a maximal ideal. Especially, $\max(R) \neq \emptyset$.

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 $I = aR$.

$\square$

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

<u>Claim 1:</u> Chains in Ω have upper bounds.

<u>Proof:</u> 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. $I = \langle a_1, ..., a_n \rangle$. Then there exists $Q \in \Sigma$ such that $a_1, ..., a_n \in Q$, which means $I \subseteq Q \subseteq I$, that is $I = Q$. Thus Q is finitely generated, contradiction. $\blacksquare$

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.

<u>Claim 2:</u> P is a prime ideal.

<u>Proof:</u> Suppose to the contrary that there exist $a, b \in R \setminus P$ s.t. $ab \in P$. Since $P + Ra \subsetneq P$, then $P \notin \Omega$, that is $P + Ra$ is finitely generated. Let $P + Ra = \langle p_1 + c_1 a, ..., p_k + c_k a \rangle$ with $p_i \in P$, $c_i \in R$. Consider $J = \{y \in R \mid ya \in P\} \subseteq R$, which is an ideal[1]. We have $P \subsetneq P + Rb \subseteq J$, where the last inclusion is immediate to check. Therefore J is finitely generated as well, i.e. $J = \langle b_1, ..., b_l \rangle$ for some $b_1, ..., b_l \in R$. We now want to show that $P = \langle p_1, ..., p_k, b_1 a, ..., b_l a \rangle$, which contradicts the fact that P is not finitely generated. The "$\supseteq$" is trivial. In order to prove "$\subseteq$", let $x \in P$. Since $P \subseteq P + aR$, we have

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

---

[1]More 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 $\mu_1, ..., \mu_l \in R$. Finally we get

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

■

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

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 $P \in \text{Spec}(R)$, $I_1, ..., I_k \lhd R$ and $\bigcap_{j=1}^{k} I_j \subseteq P$, then $I_j \in P$ for some $j \in \{1, ..., k\}$.

2. Let $I, P_1, ..., P_k \lhd R$ with $I \subseteq \bigcup_{j=1}^{k} P_j$. If $P_1, ..., P_k$ are prime, then $I \subseteq P_j$ for some $j \in \{1, ..., k\}$.

Proof.

1. Remember that $I_1 \cdot ... \cdot I_k \subseteq I_1 \cap ... \cap I_k$, thus $I_1 \cdot ... \cdot I_k \subseteq P$, 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 WLOG $a_1 + a_2 \in P_1$. 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

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

   then the statement follows by the induction hypothesis. So we may assume WLOG (towards a contradiction) that for all $j \in \{1, ..., k\}$ there exist

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

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

$\square$

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

1. If $Q \lhd S$ is prime, then $f^{-1}[Q] \lhd R$ is prime.

2. If f is surjective and $Q \lhd S$ 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

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

is a local ring.

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 $j = 1, ..., m$. The following holds:

1. $Q_1 \cap ... \cap Q_{m-1}$ and Q_m are comaximal.

2. $Q_1 \cap ... \cap Q_m = Q_1 \cdot ... \cdot Q_m$.

3. (Chinese Reminder Theorem) The map

$$\varphi \colon R \to \prod_{i=1}^{m} R/Q_i$$
$$a \mapsto (a + Q_1, ..., a + Q_m)$$

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

Proof.

1. Suppose $m \geq 3$ and define $Q = Q_1 \cap ... \cap Q_{m-1}$. Assume to the contrary that Q and Q_n are not comaximal. Then there is a maximal ideal $\mathfrak{M}$ with $Q + Q_n \subseteq \mathfrak{M}$. Then $Q \subseteq \mathfrak{M}$, and thus by 3.4.1! $Q_j \subseteq \mathfrak{M}$ for some $j = 1, ..., k-1$. 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

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

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 $x_1, ..., x_m \in R$. For all $j = 1, ..., m$, the ideals Q_j and $\prod_{\substack{i=1 \\ i \neq j}}^{m} Q_i$ are comaximal (by (1)), and hence there exist $u_j \in Q_j$ and $v_j \in \prod_{\substack{i=1 \\ i \neq j}}^{m} Q_i$ such that $u_j + v_j = 1$. Therefore $v_j \equiv \delta_{ij} \mod Q_i$, for $i = 1, ..., m$, and hence

$$x := \sum_{k=1}^{m} v_k x_k \equiv x_j \mod Q_j$$

for all $j = 1, ..., m$. This means that x is a preimage for $(x_1 + Q_1, ..., x_m + Q_m)$.

$\square$

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. If M is simple, then $\mathcal{J}(M) = \{0\}$.

2. $\mathcal{J}(M) = \bigcap_{\substack{\varphi:M\to E \\ E \text{ simple}}} \ker(\varphi)$.

   Proof. If $\varphi \not\equiv 0$, then $M/\ker(\varphi) \simeq E$, hence $\ker(\varphi) \subseteq M$ is maximal. Conversely, every maximal submodule $N \subseteq M$ is the kernel of the canonical epimorphism $M \to M/N$, and M/N is simple. $\qquad\square$

3. $\mathcal{J}(\mathbb{Z}) = \bigcap_{p \in \mathbb{P}} p\,\mathbb{Z} = \{0\}$.

4. $\mathcal{J}(R) = \{x \in R \mid 1 + Rx \subseteq R^\times\}$.

   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.

   $\qquad\square$

Lemma 3.11.

1. If $\varphi : M_1 \to M_2$ 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 $\psi : M \to E$ is a homomorphism, then $\psi \circ \varphi : M_1 \to E$ 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, 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 $N = \mathcal{J}(M)$.

$\square$

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)$\Rightarrow$(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)$\Rightarrow$(a)" Let $x_1, ..., x_n \in M$ 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 $R \to M$ 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 $\mathcal{J}(K)M \subseteq \mathcal{J}(M)$ is superfluous.

$\square$

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. $\square$

3.15. Krull's intersection theorem. Let R be a noetherian ring, M a finitely generated R-module, and $I \lhd R$. 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 $\bigcap_{n \geq 0} I^n M \overset{(1)}{=} 0$ and $\bigcap_{n \geq 0} I^n \overset{(2)}{=} 0$.

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.

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

   <u>Proof:</u> 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 $a_1, ..., a_k \in I$ such that $I = \langle a_1, ..., a_k \rangle$. So there is an $h \in \mathbb{N}$ with $a_i^h M \subseteq L$ for all $i \in [1, k]$.
   By Exercise 40 we have

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

   Let $c \in I$. If $m \in \mathbb{N}$ and $M_m = \{x \in M \mid c^m x \subseteq L\}$, then $M_1 \subseteq M_2 \subseteq ...$ is an ascending chain[2], and thus there is an $n \in \mathbb{N}$ such that $M_m = M_n$ for all $m \geq n$. We claim that
   $$(c^n M + L) \cap N = IN. \qquad (*)$$

   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 $N \subseteq I^n M \subseteq L$, and thus $N \subseteq I^n M \cap N \subseteq L \cap N = IN \subseteq N$, 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 (1) follows. Equality (2) follows from (1) with $M = R$.

3. By the second point, we have $\bigcap_{n \geq 0} I^n(M/N) = 0$. Consider $\pi : M \to M/N$. Then

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

---

[2] if $c^m x \in L$, then also $c^{m+1} x \in L$, since L is a module.
[3] Observe that $[\lambda x + y] = [\lambda x] = \lambda[x]$.

$\square$

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

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

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

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

Theorem 3.18. Let $I \lhd R$. 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 $\mathfrak{p}_1, ..., \mathfrak{p}_n \in \mathbb{P}(I)$ with $\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq I$. 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 $X := \{\mathfrak{p}_1 \ldots \mathfrak{p}_n \mid n \in \mathbb{N},\ \mathfrak{p}_1, ..., \mathfrak{p}_n \in \mathbb{P}(I)\}$. Suppose towards a contradiction that for all $\mathfrak{a} \in X$ it holds $\mathfrak{a} \not\subseteq I$. Then

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

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

<u>Claim:</u> $\mathfrak{q} \in \mathrm{Spec}(R)$.

<u>Proof:</u> Suppose there are $a, b \in R \setminus \mathfrak{q}$ with $ab \in \mathfrak{q}$. Then $\mathfrak{q} + aR \notin \Sigma$ and $\mathfrak{q} + bR \notin \Sigma$. 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 $\mathfrak{q} \in \Sigma$. $\blacksquare$
By point (1), there is a $\mathfrak{p}_0 \in \mathbb{P}(I)$ with $\mathfrak{p}_0 \subseteq \mathfrak{q}$. But obviously $\mathfrak{a}_1 \mathfrak{a}_2 \in X$, 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 $\{0\} \lhd R$, 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. AND THEN???

$\square$

3.3 Hilbert's Basis Theorem and Hilbert's Nullstellensatz.

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

Proof. It suffices to show the statement for $n = 1$. 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

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

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 $n_1 \leq n_2 \leq ...$ and $\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq ...$ is an ascending chain of ideals.

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

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

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

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

Corollary 3.20. Let $R \subseteq S$ be commutative rings, with S finitely generated on R as a ring (i.e. there are $c_1, ..., c_n \in S$ such that $S = R[c_1, ..., c_n]$). 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

$$\Phi_{c_1,...,c_n}^{X_1,...,X_n} \colon R[X_1, \ldots, X_n] \to R[c_1, \ldots, c_n] = S$$
$$X_i \mapsto c_i.$$

By Theorem 3.19, $R[X_1, ..., X_n]$ 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

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

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 $I \in \mathrm{Spec}(R)$, 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 $b^n \in I$. It follows that

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

$\square$

Proposition 3.23. Let $I \lhd R$ 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 $J \lhd R$ is finitely generated and $J \subseteq \sqrt{I}$, then there is an $m \in \mathbb{N}$ such that $J^m \subseteq I$.

3. $\sqrt{0} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p} = \bigcap_{\mathfrak{m} \in \max(R)} \mathfrak{m} = \mathcal{J}(R)$. $\sqrt{0}$ is called *nilradical* of R.

38

Proof.

1. We will show
$$\sqrt{I} \overset{(i)}{\subseteq} \bigcap_{\mathfrak{p} \in \mathcal{V}(I)} \mathfrak{p} \overset{(ii)}{\subseteq} \bigcap_{\mathfrak{p} \in \mathbb{P}(I)} \mathfrak{p} \overset{(iii)}{\subseteq} \sqrt{I}.$$

   (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 $\mathfrak{p}_0 \in \mathcal{V}(I)$ 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
   $$I \in \Omega = \{J \lhd R \mid J \cap S = \emptyset, \ I \subseteq J\}.$$
   By Krull's Existence Theorem, Ω has a maximal element $\mathfrak{p} \in \mathrm{Spec}(R)$. 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 $J =_R \langle x_1, ..., x_k \rangle$. Then 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 $\lambda_1, ..., \lambda_k \in R$, and thus a^{nk} is a sum of products of nk factors of $\{\lambda_1 x_1, ..., \lambda_k x_k\}$ and hence $a^{nk} \in I$.

3. This follows from (1), since $\mathfrak{p} \in \mathrm{Spec}(R)$ contains zero and since every maximal ideal is prime.

$\square$

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

1. Let $Z \subseteq K[X_1, ..., X_n]$. We denote with $\mathcal{V}_L(Z)$ the set
$$\mathcal{V}_L(Z) := \{\mathbf{X} \in L^n \mid \forall f \in Z \colon f(x) = 0\} \subseteq L^n,$$
   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 $f_1, ..., f_m \in K[X_1, ..., X_n]$ such that V is the set of solutions of the system
$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$
   in L^n, i.e. if $V = \mathcal{V}_L(\{f_1, ..., f_m\})$.

Theorem 3.25. Let $K \subseteq L$ be fields and $Z \subseteq K[X_1, ..., X_n]$. 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 $f(\mathbf{X}) = \sum_{i=1}^{k} g_i(x) h_i(x) = 0$, 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

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

$\square$

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

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

is called *vanishing ideal of* V.

Theorem 3.27 (Field-theoretic version of Hilbert's Nullstellensatz)**.** Let K be a field and $A = K[x_1, ..., x_n]$ 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 K-homomorphism $A \to \overline{K}$. If A is a field, then A/K is algebraic.

Proof. Bosch (Algebra II, Paragraph 39). $\square$

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

1. $\mathfrak{m} = \langle X_1 - a_1, ..., X_n - a_n \rangle \subseteq K[\mathbf{X}]$ is a maximal ideal such that $\mathcal{V}_K(\mathfrak{m}) = \{\mathbf{a}\} \subseteq K^n$ and $\mathcal{J}(\{a\}) = \mathfrak{m}$.

2. If K is algebraically closed and $\mathfrak{m} \lhd K[\mathbf{X}]$ is maximal, then there are $b_1, ..., b_n \in K$ such that $\mathfrak{m} = \langle X_1 - b_1, ..., X_n - b_n \rangle$.

Proof. We consider the valuation homomorphism

$$\varphi := \Phi_{a_1, ..., a_n}^{X_1, ..., X_n} : K[X_1, \ldots, X_n] \to K$$
$$X_i \mapsto a_i.$$

Then $K[\mathbf{X}]/\ker(\varphi) \simeq K$, thus $\ker(\varphi) \in \max(K[\mathbf{X}])$ and $\langle X_1 - a_1, ..., X_n - a_n \rangle \subseteq \ker(\varphi)$. We want to show that equality holds.

Every $f \in K[\mathbf{X}]$ has a unique representation of the form

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

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

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

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

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

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 $I \lhd R$ with $I \neq R$, then $\mathcal{V}_L(I) \neq \emptyset$.

2. If $I \lhd R$, then $\mathcal{J}(\mathcal{V}(I)) = \sqrt{I}$. The maps

$$\{K - \text{variety}, V \subseteq L^n\} \to \{\text{radical ideals of } R\}$$
$$V \mapsto \mathcal{J}(V)$$
$$\mathcal{V}_L(I) \leftmapsto I$$

   are bijective and are each other's inverse.

Proof.

1. <u>Special case:</u> $L = K$. Since $I \neq R$ there is a maximal ideal $\mathfrak{m} = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ with $I \subseteq \mathfrak{m}$, and thus $\{\mathbf{a}\} = \mathcal{V}_L(\mathfrak{m}) \subseteq \mathcal{V}_L(I)$.
   <u>General case:</u> 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

$$\Phi : K[\mathbf{X}] \to K[\mathbf{X}]/\mathfrak{m}$$
$$X_i \mapsto \xi_i := X_i + \mathfrak{m}$$

   is a ring epimorphism, and thus $A = K[\xi_1, ..., \xi_n]$ is a finitely generated K-algebra. By 3.27, A/K is algebraic, and thus there is a K-homomorphism $\varphi : A \to L$. Then

$$\Big(\varphi(\xi_1), \ldots, \varphi(\xi_n)\Big) \in L^n$$

is a root of $\mathfrak{m}$, and thus of I. (If $f \in \mathfrak{m}$, then $f\Big(\varphi(\xi_1), \dots, \varphi(\xi_n)\Big) = \varphi\Big(f(x_1, \dots, x_n)\Big) =$??? $= 0$.)

2. <u>Claim 1:</u> $\mathcal{J}(V)$ is a radical ideal.

<u>Proof:</u> 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. $f \in \mathcal{J}(V)$. $\blacksquare$

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

<u>Proof:</u> Let $\mathfrak{U} \in \mathcal{V}_L(\mathfrak{g})$ with $\mathfrak{g} \lhd K[\mathbf{X}]$. 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 $\mathcal{V}_L(\mathfrak{g}) \supseteq \mathcal{V}_L(\mathcal{J}(\mathcal{V}_L(\mathfrak{g})))$. $\blacksquare$

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

<u>Proof:</u> "$\supseteq$" 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.
"$\subseteq$" Conversely, let $0 \neq f \in \mathcal{J}(\mathcal{V}_L(I))$. Consider

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

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 $p_1, \dots, p_{s+1} \in K[\mathbf{X}, I]$ such that

$$1 = \sum_{i=1}^{s} f_i p_i + p_{s+1}(fT - 1).$$

We consider the homomorphism

$$\varphi := \Phi_{(X_1, \dots, X_n, \frac{1}{f})}^{(X_1, \dots, X_n, T)} : K[\mathbf{X}, T] \to K(X_1, \dots, X_n)$$
$$X_i \mapsto X_i$$
$$T \mapsto \frac{1}{f}.$$

Then

$$1 = \sum_{i=1}^{s} \varphi(p_i) f_i,$$

42

and we have $\varphi(p_i) = q_i/f^{m_i}$, where $q_i \in K[\mathbf{X}]$, $m_i \in \mathbb{N}$. For $m = \max\{m_1, ..., m_s\}$ we obviously get

$$f^m \in \langle f_1, \ldots, f_s \rangle \subseteq I,$$

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 $\cdot : A \times A \to A$ 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 $R[X_1, ..., X_n]$ is a commutative R-algebra.

2. If A is an R-algebra, then $\varepsilon : R \to A$, $\lambda \mapsto \lambda 1_A$ is a ring homomorphism, and for all $\lambda \in R$ and $a \in A$, $\varepsilon(\lambda)a = \varepsilon(\lambda a)$.

   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

   $$\varepsilon(\lambda)a = (\lambda 1_A)a = \lambda(1_A a) = \lambda(a 1_A) = a(\lambda 1_A) = a\varepsilon(\lambda).$$

   $\square$

3. Conversely, let A be a ring and $\varepsilon : R \to A$ 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 $\varepsilon : R \to A$ 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 $\varepsilon_1 : R \to A_1$ and $\varepsilon_2 : R \to A_2$. A ring homomorphism $f : A_1 \to A_2$ 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 $f : A_1 \to A_2$ is a ring homomorphism. Then f is an R-algebra homomorphism if and only if $f_{|R} = \mathrm{id}_R$.

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 $f(\lambda a) = f(\lambda)f(a) = \lambda f(a)$.

$\square$

5. If R is a ring, then there is exactly one ring homomorphism $\varepsilon : \mathbb{Z} \to R$ (namely, $\varepsilon(m) = m 1_R$). Thus R is a $\mathbb{Z}$-algebra.

More notations and conventions.

1. Let $0 \neq R \supseteq S$ commutative rings with S an overring. Then $R \supseteq S$, indicated also S/R, is called a *ring extension*.
For all $\mathfrak{p} \in \mathrm{Spec}(S)$ we have $\mathfrak{p} \cap R \in \mathrm{Spec}(R)$.
For any $C \subseteq S$, let $[C] = \{c_1 \cdot \ldots \cdot c_n \mid n \in \mathbb{N}_0, c_1, ..., c_n \in C\}$ 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 $\varphi_1, \varphi_2 : S \to S'$ are ring homomorphism with $\varphi_{1|R \cup C} = \varphi_{2|R \cup C}$, then $\varphi_1 = \varphi_2$.

2. Let R a commutative ring, A a commutative R-algebra and $\varepsilon : R \to A$ 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 and $n \in \mathbb{N}$ and an epimorphism $R[X_1, ..., X_n] \to A$.
   - There exist $n \in \mathbb{N}$, $x_1, ..., x_n \in A$ with $A = \varepsilon[R][x_1, ..., x_n]$, i.e. A is the smallest subring of A which contains $\varepsilon[R] \cup \{x_1, ..., x_n\}$.

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 $a_0, ..., a_{n-1} \in R$ such that $x^n + a_{n_1} x^{n-1} + ... + a_0 = 0$. The latter is called an *integral equation* of x/R.

2. The *integral closure of R in S* is $\mathrm{cl}_S(R) = \{x \in S \mid x \text{ is integral}/R\}$.

3. A subset $S' \subseteq S$ is called *integral/R* if $S' \subseteq \mathrm{cl}_S(R)$.

4. R is called *integrally closed in S* if $\mathrm{cl}_S(R) = R$.

5. If R is a domain with $\mathsf{q}(R) = K$, then R is called *integrally closed* if $\mathrm{cl}_K(R) = R$.

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*. $\overline{\mathbb{Z}} = \mathrm{cl}_{\overline{\mathbb{Q}}}(\mathbb{Z}) = \mathrm{cl}_{\mathbb{C}}(\mathbb{Z})$ is the *ring of all algebraic integers*.

3. Every field is integrally closed.

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 $\mathrm{Ann}_{R[x]}(M) = 0$ and M is a finitely generated R-module.

Proof.

(a)⇒(b) Let $n \in \mathbb{N}$, $a_{n-1}, ..., a_0 \in R$ such that $x^n + a_{n-1}x^n + ... + a_0 = 0$. By definition we have

$$R[x] = \left\{ \sum_{j=0}^{k} c_j x^j \;\middle|\; k \in \mathbb{N}, c_0, ..., c_k \in R \right\}$$

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 "⊇" is trivial. We want to prove "⊆". It is sufficient to show that $x^k \in_R \langle \{ x^j \mid j \in [0, n-1] \} \rangle$ for every $k \in \mathbb{N}$. We proceed by induction. If $k \leq n-1$ the assertion is clearly true. Let $k \geq n$ and suppose $\{ x^0, ..., x^{k-1} \} \in_R \langle \{ x^j \mid j \in [0, n-1] \} \rangle$. Then

$$x^k = x^{k-n}x^n = x^{k-n}(-a_{n-1}x^n - ... - a_0) =$$
$$- a_{n-1}x^{k-1} - ... - a_0 x^{k-n} \in_R \langle \{ x^j \mid j \in [0, n-1] \} \rangle.$$

∎

(b)⇒(c) $S' = R[x]$ has the required property.

(c)⇒(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)⇒(a) Let $M =_R \langle m_1, ..., m_n \rangle$ which is also an $R[x]$-module. Thus $xM \subseteq M$. Therefore, for all $i \in [1, n]$ there are $r_{i,1}, ..., r_{i,n} \in R$ 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

$$A^{\#} A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \underbrace{\det(A)}_{\in R} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

where $A^{\#}$ is the adjugate matrix[1] of A. Since $\mathrm{Ann}_{R[x]}(M) = 0$ by hypothesis, we get $\det(A) = 0$. Thus there are $w_0, ..., w_{n-1} \in R$ such that

$$0 = \det(A) \overset{2}{=} (-1)^n x^n + w_{n-1} x^{n-1} + \ldots + w_0,$$

which is an integral equation for x.

$\square$

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 $M =_S \langle x_1, ..., x_n \rangle$ and $S =_R \langle a_1, ..., a_m \rangle$. We claim that

$$M =_R \langle a_j x_j \mid j \in [1, m], i \in [1, n] \rangle.$$

Let $x \in M$. Then there are $s_1, ..., s_n \in S$ such that $x = \sum_{i=1}^n s_i x_i$. For all $i \in [1, n]$ there are $\lambda_{i,1}, ..., \lambda_{i,m} \in R$ such that $s_i = \sum_{j=1}^m \lambda_{i,j} a_j$. Thus

$$x = \sum_{i=1}^n s_i x_i = \sum_{i=1}^n \left(\sum_{j=1}^m \lambda_{i,j} a_j \right) x_i = \sum_{i=1}^n \sum_{j=1}^m \lambda_{i,j} (a_j x_i).$$

$\square$

Examples.

1. $M = \mathbb{C}$, $R = \mathbb{R} \subseteq \mathbb{C} = S$.

2. Field extension: $K \subseteq L \subseteq M$.

Corollary 4.5. Let $R \subseteq S$ be a ring extension and $x_1, ..., x_n \in S$ with $S = R[x_1, ..., x_n]$. The following are equivalent:

(a) $\{x_1, ..., x_n\} \subseteq \mathrm{cl}_S(R)$.

(b) S is a finitely generated R-module.

(c) S is integral over R.

Proof.

---

[1] If 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.

[2] Observe 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, $S' = R[x_1, ..., x_{n-1}]$ is a finitely generated R-module. Since x_n is integral$/R$, x_n is integral$/S'$. Again by induction hypothesis, $S'[x_n] = R[x_1, ..., x_n]$ 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(c), every $x \in S$ is integral$/R$.

(c)$\Rightarrow$(a) By definition. $\qquad\square$

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 $R \subseteq \mathrm{cl}_S(R) \subseteq S$, and $\mathrm{cl}_S(R)$ 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 $n \in \mathbb{N}_0$, $b_0, ..., b_{n-1}$ such that $x^n + b_{n-1}x^{n-1} + ... + b_0$. Thus x is integral over $S' = R[b_0, ..., b_{n-1}]$, and therefore $S'[x]$ is a finitely generated S'-module by Theorem 4.3. Since $b_0, ..., b_{n-1}$ 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 $\mathrm{cl}_S(R) \subseteq S$ is a subring.
   Let $x, y \in \mathrm{cl}_S(R)$. 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 twice.

   (ii) We want to prove that $\mathrm{cl}_S(R)$ is integrally closed in S. Let $x \in S$ be integral$/ \mathrm{cl}_S(R)$. Since $\mathrm{cl}_S(R)$ is integral$/R$, by point 1(a) we have that x is integral$/R$, i.e. $x \in \mathrm{cl}_S(R)$.

$\qquad\square$

Theorem 4.7. Let R be an integrally closed domain with $\mathsf{q}(R) = K$, 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 "⇐" is obvious. We want to show "⇒". Let N/L be a splitting field of f over L. So

$$f = \prod_{i=1}^{n}(X - x_i) \quad \text{with } x_1, ..., x_n \in N.$$

We can assume $x = x_1$. Then, for all $i \in [1, n]$, there is a K-isomorphism

$$\varphi_i : K[x] \to K[x_i] \subseteq N, \quad \varphi_i(x) = x_i.$$

By hypothesis, there exist $a_0, ..., a_{d-1} \in R$ such that $x^d + a_{d-1}x^{d-1} + ... + a_1x + a_0 = 0$. Therefore

$$\varphi_i(x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0) = x_i^d + a_{d-1}x_i^{d-1} + \ldots + a_1x_i + a_0 = 0,$$

i.e. x_i is integral$/R$. Thus the coefficients of f are in K (why??? I just know that every x_i is in N and is integral$/R$, nothing more!) and they are integral$/R$, which means that they are in R since R is integrally closed. That is, $f \in R[X]$. $\square$

Corollary 4.8. Let R be an integrally closed domain, $K = \mathfrak{q}(R)$, $f \in R[X] \setminus R$ 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. <u>Claim:</u> If $p \in K[X]$ is monic and irriducible with $p|f$ in $K[X]$, then $p \in R[X]$.
<u>Proof:</u> 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. ∎
Since $K[X]$ is a UFD, the main statement follows. $\square$

Definition 4.9. Let $0 \neq R$ be a commutative ring and $\mathfrak{g} \in \mathrm{Spec}(R)$. Then

$$h(\mathfrak{g}) := \sup\{l \in \mathbb{N}_0 \mid \text{ there are prime ideals } \mathfrak{g} = \mathfrak{g}_0 \supsetneq \ldots \supsetneq \mathfrak{g}_l\}$$

is called the *height of* $\mathfrak{g}$, and

$$\dim(R) := \sup\{h(\mathfrak{g}) \mid \mathfrak{g} \in \mathrm{Spec}(R)\}$$

is called the (Krull) *dimension of R*.

Remarks.

1. R is a domain if and only if $0 \in \mathrm{Spec}(R)$. 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 $g \in P(xR)$, where $P(xR)$ is the family of minimal prime ideals lying in xR. Then $h(g) \leq 1$. In particular, if R is a PID, then $\dim(R) = 1$.

Theorem 4.10 (Cohen-Seidenberg)**.** Let $R \subseteq S$ be an integral ring extension. The following hold:

1. (Incomparability) Let $\mathfrak{p} \in \mathrm{Spec}(S)$ and $\mathfrak{a} \lhd S$ 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 $\mathfrak{g} \in \mathrm{Spec}(R)$ and $\mathfrak{a} \lhd S$ with $\mathfrak{a} \cap R \subseteq \mathfrak{g}$ there is a $\mathfrak{p} \in \mathrm{Spec}(S)$ such that $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap R = \mathfrak{g}$. In particular, the map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$, $\mathfrak{p} \mapsto \mathfrak{p} \cap R$, is surjective.

3. (Going up) Let $\mathfrak{g}_0, \mathfrak{g} \in \mathrm{Spec}(R)$ and $\mathfrak{p}_0 \in \mathrm{Spec}(S)$ such that $\mathfrak{p}_0 \cap R = \mathfrak{g}_0 \subseteq \mathfrak{g}$. Then there is a $\mathfrak{p} \in \mathrm{Spec}(S)$ such that $\mathfrak{p}_0 \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap R = \mathfrak{g}$.

4. $\max(S) = \{\mathfrak{p} \in \mathrm{Spec}(S) \mid \mathfrak{p} \cap R \in \max(R)\}$. 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 $a_0, ..., a_{n-1} \in R$ with

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathfrak{p}.$$

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

$$a_0 = p - x(x^{n-1} + \ldots + a_1) \in \mathfrak{a} \cap R = \mathfrak{p} \cap R \subseteq \mathfrak{p},$$

hence $x(x^{n-1} + \ldots + a_1) \in \mathfrak{p}$. By minimality $x^{n-1} + \ldots + a_1 \notin \mathfrak{p}$, whereby $x \in \mathfrak{p}$.

2. Let $\mathfrak{g} \in \mathrm{Spec}(R)$ and $\mathfrak{a} \lhd S$ 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 $\{\mathfrak{c} \lhd S \mid \mathfrak{a} \subseteq \mathfrak{c}, \mathfrak{c} \cap (R \setminus \mathfrak{g}) = \emptyset\}$ has a maximal element $\mathfrak{p}$. Then $\mathfrak{p} \in \mathrm{Spec}(S)$ with $\mathfrak{a} \subseteq \mathfrak{p}$ 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

$$s^n + a_{n-1}s^{n-1} + \ldots + a_0 = 0$$

an integral equation of s over R. Then

$$u^n(s^n + a_{n-1}s^{n-1} + \ldots + a_0) = (us)^n + a_{n-1}u(us)^{n-1} + \ldots + a_1 u^{n-1}(us) + a_0 u^n = 0,$$

and since $us \equiv x \mod \mathfrak{p}$ we get

$$x^n + a_{n-1}ux^{n-1} + \ldots + a_1 u^{n-1}x + a_0 u^n \in \mathfrak{p} \cap R \subseteq \mathfrak{g}.$$

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 $\mathfrak{p} \in \mathrm{Spec}(S)$. 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 $\mathfrak{m} \in \mathrm{Spec}(S)$ 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 $\mathfrak{p} \in \mathrm{Spec}(S)$ 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 $\mathfrak{g}_0 \subsetneq \mathfrak{g}_1 \subsetneq \ldots \subsetneq \mathfrak{g}_n$ be a sequence in $\mathrm{Spec}(R)$. By point (2), there is a $\mathfrak{p}_0 \in \mathrm{Spec}(S)$ such that $\mathfrak{p}_0 \cap R = \mathfrak{g}_0$. Applying point (3) repeatedly, we obtain a sequence $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ in $\mathrm{Spec}(S)$ with $\mathfrak{p}_i \cap R = \mathfrak{g}_i$ for all $i \in [1, n]$. Thus $\dim(S) \geq \dim(R)$. Conversely, if $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ is a sequence in $\mathrm{Spec}(S)$, then $\mathfrak{p}_0 \cap R \subsetneq \ldots \subsetneq \mathfrak{p}_n \cap R$ 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

$$\mathcal{O}_L = \mathrm{cl}_L(\mathbb{Z})$$

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 $\mathsf{q}(\mathcal{O}_L) = L$. Let $x \in L$. Then there exist $a_n, ..., a_0 \in \mathbb{Z}$ with

$$a_n x^n + \ldots + a_0 = 0.$$

Multiplying by a_n^{n-1} we obtain that

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \ldots + a_0 a_n^{n-1} = 0.$$

Thus $a_n x$ is integral$/\,\mathbb{Z}$, which means $a_n x \in \mathcal{O}_L$. Hence $x \in \mathsf{q}(\mathcal{O}_L)$. $\qquad\square$

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 $\dim_K(A) = n$. For $\lambda \in A$, let $\mu_\lambda : A \to A$ be defined by
$$\mu_\lambda(a) = \lambda a.$$
Then $\mu_\lambda \in \mathrm{End}_K(A)$, and we define

$$\begin{aligned}
N_{A/K} &: A \to K &\quad \text{and} \quad \mathrm{Tr}_{A/K} &: A \to K \\
\lambda &\mapsto N_{A/K}(\lambda) := \det(\mu_\lambda) & \lambda &\mapsto \mathrm{Tr}_{A/K}(\lambda) := \mathrm{Tr}(\mu_\lambda)
\end{aligned}$$

Remark. Let $\mathbf{u} = (u_1, ..., u_n)$ be a K-basis of A and let $\mathcal{M}_{\mathbf{u},\mathbf{u}}(\mu_\lambda)$ be such that

$$(\lambda u_1, ..., \lambda u_n) = (u_1, .., u_n)\mathcal{M}_{\mathbf{u},\mathbf{u}}(\mu_\lambda).$$

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 $\varphi \in \mathrm{End}_K(A)$ 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. $\mathrm{Tr}_{A/K}(\alpha + \beta) = \mathrm{Tr}_{A/K}(\alpha) + \mathrm{Tr}_{A/K}(\beta)$.

4. $\mathrm{Tr}_{A/K}(\lambda\alpha) = \lambda\,\mathrm{Tr}_{A/K}(\alpha)$.

5. $\mathrm{Tr}_{A/K}(\lambda) = n\lambda$.

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 $\mathbf{u} = (u_1, ..., u_n)$ is a K-basis of A, then $\mu_\lambda(u_i) = \lambda u_i$ for all $i \in [1, n]$, and $\mathcal{M}_{\mathbf{u},\mathbf{u}}(\mu_\lambda) = \lambda I$.

3., 4. Observe that
$$\mathcal{M}_{\mathbf{u},\mathbf{u}} \colon \mathrm{End}_K(A) \to M_n(K)$$
$$\varphi \mapsto \mathcal{M}_{\mathbf{u},\mathbf{u}}(\varphi)$$

is a K-algebra isomorphism, i.e. $\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$ and $\mathrm{Tr}(\lambda A) = \lambda\,\mathrm{Tr}(A)$.

$\square$

For the rest of this Section, let L/K be a finite separable field extension of degree $[L : K] = n$, and let $\overline{K}$ be an algebraically closed field with $K \subseteq L \subseteq \overline{K}$.
We will use the following result, which should be known from previous courses:
Theorem. For every K-homomorphism $K \to K \hookrightarrow \overline{K}$ there exist precisely n distinct lifts $\sigma : L \to \overline{K}$.
This means $|\mathrm{Hom}_K(L, \overline{K})| = [L : K]$. We set $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, ..., \sigma_n\}$.

Lemma 4.14. Let $\alpha \in L$, $f = X^r + a_{r-1}X^{r-1} + \ldots + a_0 \in K[X]$ the minimal polynomial of α over K and $[L : K(\alpha)] = s$. Then

1. $N_{L/K}(\alpha) = \left((-1)^r a_0\right)^s$.

2. $\mathrm{Tr}_{L/K}(\alpha) = -s\, a_{r-1}$.

Proof. We have $n = [L : K] = [L : K(\alpha)][K(\alpha) : K] = s\,r$ and $(1, \alpha, ..., \alpha^{r-1})$ is a K-basis of $K(\alpha)/K$. If $\mathbf{v} = (v_1, ..., v_s)$ 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

$$\mu_\alpha(v_i\alpha^j) = v_i\alpha^{j+1} \text{ for } j \in [0, r-2] \quad \text{and} \quad \mu_\alpha(v_i\alpha^{r-1}) = v_i(-a_0 - \dots - a_{r-1}\alpha^{r-1}).$$

Since (by abuse of notation), $\mu_\alpha(\mathbf{u}) = \mathcal{M}_{\mathbf{u},\mathbf{u}}(\mu_\alpha)$, 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

$$A_1 = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ 0 & 0 & \dots & 0 & \vdots \\ 0 & 0 & \dots & 1 & -a_{r-1} \end{pmatrix}.$$

Therefore

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(A) = s\,\mathrm{Tr}(A_1) = s(-a_{r-1})$$

and

$$N_{L/K}(\alpha) = \det(A) = (\det(A_1))^s = ((-1)^{r+1}(-a_0) \cdot 1)^s = ((-1)^r a_0)^s.$$

$\square$

Lemma 4.15. For every $\alpha \in L$ we have

$$N_{L/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) \quad \text{and} \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

Proof. We have $K \subseteq L \subseteq \overline{K}$, $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, ..., \sigma_n\}$. Let $\alpha \in L$, $f = X^r + a_{r-1}X^{r-1} + ... + a_0 \in K[X]$ 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 WLOG $\alpha = \alpha_1$. Since α is separable, $\alpha, \alpha_2, ..., \alpha_r$ are pairwise distinct. Thus there are r distinct K-monomorphism

$$\tau_\nu : K(\alpha) \to \overline{K} \quad \text{s.t.} \quad \tau_\nu(\alpha) = \alpha_\nu, \quad \text{with } \nu \in [1, r].$$

By the theorem discussed above, since $L/K(\alpha)$ is separable, we have

$$|\{\psi : L \to \overline{K} \mid \psi \text{ is a } K\text{-homomorphism, } \psi_{|K(\alpha)} = \tau_\nu\}| = [L : K(\alpha)] = s.$$

If $\tau_{\nu,1}, ..., \tau_{\nu,s}$ are the lifts of τ_ν, then

$$\{\sigma_1, ..., \sigma_n\} = \{\tau_{\nu,j} \mid \nu \in [1, r], j \in [1, s]\}.$$

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

$$\sum_{i=1}^{n} \sigma_i(\alpha) = \sum_{\nu=1}^{r}\sum_{j=1}^{s} \tau_{\nu,j}(\alpha) = s\sum_{\nu=1}^{r} \alpha_\nu = s(-a_{r-1}) = \mathrm{Tr}_{L/K}(\alpha),$$

where the two last equalities hold by Lemma 4.14. $\qquad \square$

Definition 4.16. If $\mathbf{u} = (u_1, ..., u_n)$ is a basis of L/K, then

$$\Delta(\mathbf{u}) = \det\left(\mathrm{Tr}_{L/K}(u_i u_j)\right)_{1 \le i,j \le n}$$

is called the *discriminant of* $\mathbf{u}$.

Theorem 4.17. Let $\mathbf{u} = (u_1, ..., u_n)$ be a basis of L/K. The following hold:

1. If $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, ..., \sigma_n\}$, then $\Delta(\mathbf{u}) = \det\left(\sigma_i(u_j)\right)^2_{1 \le i,j \le n}$.

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 $L = K(\alpha)$, $\mathbf{u} = (1, \alpha, ..., \alpha^{n-1})$, and $\alpha, \alpha_2, ..., \alpha_n$ are the K-conjugates of α, then $\Delta(\mathbf{u}) = \prod_{i<j}(\alpha_i - \alpha_j)^2$.

4. We have $\Delta(\mathbf{u}) \ne 0$ and $\mathrm{Tr}_{L/K} : L \to K$ is not the zero map.

5. There is a basis $\mathbf{u}^* = (u_1^*, ..., u_n^*)$ of L/K with $\mathrm{Tr}_{L/K}(u_i u_j^*) = \delta_{i,j}$ 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

$$\mathrm{Tr}_{L/K}(u_i u_j) = \sum_{\nu=1}^{n} \sigma_\nu(u_i)\sigma_\nu(u_j) = \Big(\sigma_1(u_i), \ldots, \sigma_n(u_i)\Big) \begin{pmatrix} \sigma_1(u_j) \\ \vdots \\ \sigma_n(u_j) \end{pmatrix}.$$

Thus

$$\Big(\mathrm{Tr}_{L/K}(u_i u_j) \Big)_{1 \le i,j \le n} = A^T A,$$

where $A = \Big(\sigma_i(u_j) \Big)_{1 \le i,j \le n}$, whereby follows the assertion.

$\square$

Definition 4.18.

Definition 4.19.

Definition 4.20.

Definition 4.21.

Definition 4.22.

Definition 4.23.

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 $0 \neq P \lhd \mathcal{O}_L$ 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 $P_1, ..., P_g \in \mathrm{Spec}(\mathcal{O}_L)$. 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 $e_1 = ... = e_j = 1$, 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 $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$, then $\bar{\sigma} \in \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$; σ is called real if $\sigma(L) \subseteq \mathbb{R}$ and complex otherwise. Let $\sigma_1, ..., \sigma_r : L \to \mathbb{C}$ be the real embeddings, and

$$\sigma_{r+1}, ..., \sigma_{r+s}, \overline{\sigma_{r+1}}, ..., \overline{\sigma_{r+s}} : L \to \mathbb{C}$$

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 $0 \neq I \lhd R$ is invertible if there is $J \lhd R$ s.t. $IJ \in \mathcal{H}(R)$).

We have a monoid isomorphism $R^{\circ}/R^{\times} \to \mathcal{H}(R)$, $aR^{\times} \mapsto aR$, and

$$K^{\times}/R^{\times} = \mathsf{q}(R^{\circ}/R^{\times}) \simeq \mathsf{q}(\mathcal{H}(R)) = \{aR \mid a \in K^{\times}\}.$$

Then $\mathcal{F}(R)^{\times} := \mathsf{q}(\mathcal{I}^{\times}(R))$ is called the group of invertible fractional ideals,

$$\mathrm{Pic}(R) = \mathcal{F}(R)^{\times} / \mathsf{q}(\mathcal{H}(R))$$

is the Picard group of R and we have an exact sequence

$$1 \to R^{\times} \hookrightarrow K^{\times} \xrightarrow{f} \mathcal{F}(R)^{\times} \to \mathrm{Pic}(R) \to 1$$

where $f(x) = xR$. If R is Dedekind, then $\mathcal{F}^{\circ}(R) = \mathcal{F}^*(R)$, and $\mathrm{Pic}(R) = \mathrm{cl}(R)$ is called the ideal class group of R.

Theorem. $\mathrm{Pic}(\mathcal{O}_L)$ 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 $\operatorname{char}(K) \neq 2$. 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 irriducible. Thus $d \in K^\times \setminus K^{\times 2}$ and it remains to show:

<u>Claim:</u>   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 $d_1 K^{\times 2} = d_2 K^{\times 2}$.

<u>Proof:</u> ($\Rightarrow$) 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 sice $\alpha_1 \notin K$ 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 $\operatorname{Hom}_\mathbb{Q}(K, \mathbb{C}) = \{\sigma_1, \sigma_2\}$, with $\sigma_1, \sigma, 2 : K \to \mathbb{C}$, $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$, $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$.

   (iii) For all $a, b \in \mathbb{Q}$, we have $N_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - b^2 d$ and $Tr_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a$.

2. (i) If $d \equiv 2, 3 \mod 4$, then $(1, \sqrt{d})$ is an integral basis of K, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, and $\Delta_K = 4d$.

   (ii) If $d \equiv 1 \mod 4$, 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

$$a\mathbb{Q}^{\times 2} = \varepsilon \prod_{V_p(a) \equiv 1 \mod 2} p\mathbb{Q}^{\times 2} \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2} \tag{$*$}$$

and since $\displaystyle\prod_{V_p(a) \equiv 1 \mod 2} p$ 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 $d \equiv 1 \mod 4$, 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 $N_{K/\mathbb{Q}}(\alpha) = a^2 - b^2 d$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a \in \mathbb{Z}$.
Then
$$4(a^2 - b^2 d) - (2a)^2 = (2b)^2 d \in \mathbb{Z}$$

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 $a'^2 - b'^2 d \equiv 0 \mod 4$.
<u>Case 1.</u> $d \equiv 2, 3 \mod 4$. Then $a'^2 \equiv 2b'^2 \mod 4$ or $a'^2 \equiv 3b'^2 \mod 4$. This implies that $a' \equiv b' \equiv 0 \mod 2$ and hence $\alpha \in \mathbb{Z}\langle 1, \sqrt{d'}\rangle$.
<u>Case 2.</u> $d \equiv 1 \mod 4$. Then $a'^2 \equiv b'^2 \mod 4$ and hence $a' \equiv b' \mod 2$. 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.
<u>Case 1.</u> $d \equiv 2, 3 \mod 4$.

$$\Delta_K = \Delta\left((1, \sqrt{d})\right) \overset{4.17.1}{=} \det\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d.$$

<u>Case 2.</u> $d \equiv 1 \mod 4$.

$$\Delta_K = \Delta\left(\left(1, \frac{1 + \sqrt{d}}{2}\right)\right) = \det\begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = \left(\frac{1 + \sqrt{d}}{2} - \frac{1 + \sqrt{d}}{2}\right)^2 = d.$$

$\square$

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.