1. *Extension-Contraction and the Spectrum of a Polynomial Ring*

For subsets A, B of a ring R, we define

$$AB = \{a_1b_1 + \ldots + a_nb_n \mid n \in \mathbb{N},\ a_i \in A,\ b_i \in B\}.$$

For a subset S of a commutative ring R with 1, the ideal iof R generated by the set S is SR.

$* * *$ *Extension and Contraction of Ideals* $* * *$

If $R \subseteq S$ are commutative rings then every ideal I of R defines an ideal of S by **expansion**: I^e is the ideal of S generated by I. If S is a commutative ring with 1 then $I^e = IS$. Every ideal J of S defines an ideal of R by contraction: $J^e = J \cap R$.

More generally, if $f\colon R \to S$ is a ring-homomorphism, then every $I \trianglelefteq R$ defines an ideal I^c of S: the ideal of S generated by $f(I)$. If S is a commutative ring with 1 then $I^c = f(I)S$. Every ideal J of S defines an ideal of R via contraction $J^c = f^{-1}(J)$ of R.

(When f is understood, I^e is often written as IS and J^e as $J \cap R$ by abuse of notation even if f is not injective.)

Contraction preserves the property of being a prime ideal (or a primary ideal); extension, in general, does not.

Clearly, for ideals A, B of R and C, D of S, $A \subseteq B \Rightarrow A^c \subseteq B^c$ and $C \subseteq D \Rightarrow C^e \subseteq D^e$; and $A^{ce} \subseteq A$ and $D^{ec} \supseteq D$.

Therefore, for every ring homomorphism $f\colon R \to S$, extension and contraction give a bijective correspondence between ideals of R of the form $J^c = J \cap R$ (J an ideal of S) and ideals of S of the form $I^e = IS$ (I an ideal of R). In two noteable cases, all ideals of S are of the form I^e:

- Let H be an ideal of R and $\pi\colon R \to R/H$, $\pi(r) = r + H$, the canonical projection. Then extension and contraction induce a bijection between all ideals of R/H and the ideals of R containing H. In both directions of this bijection the properties of being a prime ideal, a primary ideal, or a G-ideal are preserved. Note that for a subset S of R/H $\pi^{-1}(S) = \bigcup_{r+H \in S} r + H$.
- Let S be a multiplicative subset of R, R_S the ring of quotients with denomiators in S and $f\colon R \to R_S$ the canonical map $f(r) = r/1$ (if R has a unit element, or $f(r) = rs/s$ otherwise). Recall that f is injective whenever S contains no zero-divisors. Then extension and contraction induce a bijection between all

ideals of R_S and those ideals of R that are disjoint from S. Most importantly, if $S = R \subseteq P$, P a prime ideal, then the bijection is between all ideals of R_P and the ideals of R contained in P.

Recall that for I an ideal of R, the rings $R[x]/I[x]$ and $(R/I)[x]$ are canonically isomorphic via $a_0 + a_1 x + \ldots + a_n x^n + I[x] \mapsto (a_0 + I) + (a_1 + I)x + \ldots + (a_n + I)x^n$.

$***$ *Spectrum of a Polynomial Ring* $***$

Let R be a polynomial ring and P a prime ideal of R. Then every prime ideal Q of $R[x]$ with $Q \cap R \supseteq P$ contains $P[x]$ and is therefore of the form $\pi^{-1}(\bar{Q})$, where $\pi\colon R[x] \to R[x]/P[x] = (R/P)[x]$ is the canonical projection and $\bar{Q}$ is a prime ideal of $(R/P)[x]$. Those Q among them with $Q \cap R = P$ correspond to those $\bar{Q}$ for which $\bar{Q} \cap (R/P) = (0 + P)$.

Let D be a domain with quotient field K. Then every prime ideal Q of $D[x]$ with $Q \cap D = (0)$ is of the form $\bar{Q} \cap D[x]$, where $\bar{Q}$ is a prime ideal of $K[x]$ (and thus $\bar{Q} = (f)$, where f is an irreducible polynomial of $K[x]$.

To summarize: to determine for a given prime ideal P of R all prime ideals Q of $R[x]$ with $Q \cap R = P$: consider the polynomial ring $K_P[x]$, where K_P is the quotient field of R/P, i.e. $K_P = (R/P \setminus \{0+P\})^{-1} R/P$ for each monic irreducible $f \in K_P[x]$, consider all polynomials of $R/P[x]$ that are divisible by f in $K_P[x]$, i.e. all products fg with $g \in K_P[x]$, such that $fg \in R/P[x]$. Then the collection of all polynomials of $D[x]$ whose residue class (under the projection of coefficients from R to R/P is of the form fg (for some $g \in K_P[x]$) is a prime ideal of $D[x]$ and all prime ideals Q of $D[x]$ with $Q \cap R = P$ are of this form.

2. *Modules*

2.1 Definition. Let R be a commutative ring. An Abelian group $(A, +)$ together with a "scalar" multiplication $\cdot\colon R \times A \to A$ by elements of R is called an **R-module**, if the following conditions hold for all $r,\, s \in R$ and $a,\, b \in A$:

$(r + s)a = ra + sa$

$(rs)a = r(sa)$

$r(a + b) = ra + rb$

In addition, we will always assume that modules are **unitary**, which means that multiplication by $1 \in R$ is the identity map on A, i.e., for all $a \in A$, $1_R a = a$.

2.2 Definition. Given an R-module A, the **annihilator** of a subset B of A is $\mathrm{Ann}_R(B) = \{r \in R \mid \forall b \in B \;\; rb = 0\}$.

Clearly, $\mathrm{Ann}_R(B)$ is an ideal of R for any B. Of particular importance is the annihilator of the whole module. If $\mathrm{Ann}_R(A) = I$ for an R-module A then A can be regarded as an R/I-module by defining $(r + I)a := ra$.

2.3 Definition. An R-module A is called **faithful** if $\mathrm{Ann}_R(A) = (0)$.

2.4 Definition. A (possibly non-commutative) ring A is called an **R-algebra**, if $(A, +)$ is an R-module and the multiplication of the ring A interacts peacefully with the scalar multiplication as follows: for all $r \in R$ and $a,\, b \in A$

$$r(ab) = (ra)b = a(rb).$$

Examples of R-algebras include the polynomial ring $R[x]$ and the ring $M_n(R)$ of $n \times n$ matrices with entries in R. More generally, every ring T of which R is a subring is an R-algebra (by restriction of the ring-multiplication on T to $\cdot\colon R \times T \to T$).

Because of $rb = (r1_A)b$, an R-algebra A is faithful if and only if $\mathrm{Ann}(1_A) = (0)$, and therefore every faithful R-algebra A admits an embedding of R by $r \mapsto r1_A$. If we call $\tilde{R}$ the copy of R thus embedded in A, then, again by $rb = (r1_A)b$, the scalar multiplication of the R-algebra A is just the restriction of the ring multiplication of A to $\tilde{R} \times A$.

3. *Cayley-Hamilton and McCoy Theorems*

A little excursion into linear algebra.

For R a commutative ring, let $M_n(R)$ be the R-algebra of $n \times n$ matrices with entries in R. We denote the identity matrix by I.

3.1 Lemma. Let R be a commutative ring. For $A = (a_{ij}) \in M_n(R)$, define the **adjoint** of A as $\operatorname{adj}(A) = B = (b_{ij}) \in M_n(R)$ with $b_{ij} = (-1)^{i+j} \det(A^i_j)$, where $A^i_j \in M_{n-1}(R)$ results from A by removing the i-th column and the j-th row.

Then

$$AB = BA = (\det A)I.$$

Proof. Routine verification. □

The adjoint of a matrix can be used to give a short proof of Cayley-Hamilton's theorem. It uses the natural R-algebra homomorphism between $M_n(R[x])$ and $M_n(R)[x]$, which maps the matrix whose (i,j)-th entry is $\sum_k a_k^{(i,j)} x^k \in R[x]$, to the polynomial $\sum_k A_k x^k$, where $A_k \in M_n(R)$ is the matrix whose (i,j)-th entry is $a_k^{(i,j)}$.

If S is a non-commutative ring, such as $M_n(R)$, and we want to substitute a ring element s for the variable in $f(x) = \sum a_k x^k \in S[x]$, we must specify whether substitution happens on the right or on the left of the coefficients, i.e., if $f(s)$ means $\sum a_k s^k$ (right substitution) or $\sum s^k a_k$ (left substitution).

In any case, it is important to remember that substitution (whether right or left) is in general not a homomorphism: if $f, g \in S[x]$ and $s \in S$, it is in general not true that $(f \cdot g)(s) = f(s) \cdot g(s)$ (unless s commutes with the coefficients of f and g). One thing that does work similarly to polynomials over commutative rings is the correspondence between zeros and linear factors:

3.2 Lemma. Let S be a (possibly non-commutative) ring and $f = \sum a_k x^k \in S[x]$. For $s \in S$ define $f(s) = \sum a_k s^k$. Then $f(s) = 0$ if and only if $f(x) = g(x)(x - s)$ for some $g \in S[x]$.

Proof. If $f(s) = 0$ then $f(x) = f(x) - f(s) = \sum_k a_k x^k - \sum_k a_k s^k = \sum_k a_k (x^k - s^k) = \sum_k a_k (\sum_{j=0}^{k-1} s^j x^{k-j-1})(x - s) = g(x)(x - s)$.

If, on the other hand, $f(x) = g(x)(x - s)$ with $g(x) = \sum_{k=0}^n b_k x^k$ then $f(x) = \sum_{k=0}^n b_k x^{k+1} - \sum_{k=0}^n b_k s x^k = \sum_{k=0}^{n+1} (b_{k-1} - b_k s) x^k$ and right substitution yields $f(s) = 0$. □

3.3 Theorem (Cayley-Hamilton). Let C be a $n \times n$ matrix with entries in a commutative ring R, and $\chi(x) = \det(xI - C)$ its characteristic polynomial. Then $\chi(C) = 0$.

Proof. Let $B \in M_n(R[x])$ be the adjoint of $xI - C$ then

$$B \cdot (xI - C) = \chi(x)I.$$

Applying the R-algebra isomorphism $M_n(R[x]) \simeq M_n(R)[x]$, we get

$$B(x)(x - C) = \chi(x),$$

where $B(x) \in M_n(R)[x]$ is the polynomial corresponding to the matrix $B \in M_n(R[x])$. Now $\chi(x)$ has a factor $x - C$ in $M_n(R)[x]$, and therefore $\chi(C) = 0$. □

With the argument we used to prove Cayley-Hamilton (3.3), one can actually show a stronger result, characterizing the ideal of those polynomials in $R[x]$, which have a given matrix $C \in M_n(R)$ as a zero:

3.4 Theorem (McCoy). Let C be a $n \times n$ matrix with entries in a commutative ring R. For $1 \leq k \leq n$ let $J_k(xI - C)$ be the ideal of $R[x]$ generated by the $k \times k$ minors of $xI - C$. Then the ideal of all polynomials $f \in R[x]$ with $f(C) = 0$ is equal to the ideal quotient $(J_n(xI - C) : J_{n-1}(xI - C)) = (\chi_C(x)R[x] :_{R[x]} J_{n-1}(xI - C))$.

Proof. Since the generators of $J_{n-1}(xI - C)$, the $(n-1) \times (n-1)$-minors of $(xI - C)$, are (up to sign) the entries of $adj(xI - C)$),

$$g(x) \in (\chi(x)R[x] :_{R[x]} J_{n-1}(xI - C))$$

is equivalent to

$$g(x)adj(xI - C) \in \chi(x)M_n(R[x]).$$

Multiplying by $(xI - C)$, which, being monic, is certainly not a zero-divisor in $M_n(R)[x]$, we again get an equivalent statement:

$$g(x)\chi(x)I \in \chi(x)M_n(R[x])(xI - C).$$

We may cancel the scalar $\chi(x) \in R[x]$ (a monic polynomial - not a zero-divisor in R[x]) to arrive at the equivalent statement

$$g(x)I \in M_n(R[x])(xI - C),$$

and apply the isomorphism between $M_n(R[x])$ and $M_n(R)[x]$ to get

$$g(x) \in M_n(R)[x](x - C),$$

which is (by 3.2) equivalent to C being a zero of $g(x)$. □

From Cayley-Hamilton theorem for matrices it is possible to derive a version of Cayley-Hamilton theorem for linear operators, by associating matrices to linear operators:

Suppose M is an R-module generated by $m_1, \ldots, m_n$. Then every $b \in M$ is representable as $b = b_1 m_1 + \ldots + b_n m_n$ with (in general non-unique) $b_1, \ldots, b_n$ in R. Let $\varphi \in \mathrm{End}_R(M)$. We say that a matrix $C \in M_n(R)$ represents φ with respect to the system of generators $m_1, \ldots, m_n$, if for every $b \in M$, $b = b_1 m_1 + \ldots + b_n m_n$ implies $\varphi(b) = b'_1 m_1 + \ldots + b'_n m_n$ with $C[b_1, \ldots, b_n] = [b'_1, \ldots, b'_n]$. (We use square brackets to denote column vectors: $[b_1, \ldots, b_n]$ means the transpose of $(b_1, \ldots, b_n)$. It is easy to see that C represents φ if and only if the k-th column of C is a coordinate vector of $\varphi(m_k)$, i.e., if $\varphi(m_k) = c_{1k} m_1 + c_{2k} m_2 + \ldots + c_{nk} m_n$.

If the generators $m_1, \ldots, m_n$ are not R-linearly independent, then the matrix associated to a linear operator $\varphi \in \mathrm{End}_R(M)$ is non-unique, and not every matrix in $M_n(R)$ represents a linear operator. If C represents φ and D represents ψ, however, then $C + D$ and CD represent $\varphi + \psi$ and $\varphi \circ \psi$, respectively, and, for $r \in R$, rC represents $r\varphi$, so the set $E \subseteq M_n(R)$ of matrices representing R-endomorphisms of M is a R-subalgebra of $M_n(R)$, and there is a surjective R-algebra homomorphism $\pi \colon E \to \mathrm{End}_R(M)$, mapping every matrix in E to the endomorphism it represents. In particular, for every matrix C represening some $\varphi \in \mathrm{End}_R(M)$, restriction of π to $R[C]$ gives a surjective R-algebra homomorphism $\pi \colon R[C] \to R[\varphi]$, mapping $f(C) \in R[C]$ to $f(\varphi) \in R[\varphi]$ for every $f \in R[x]$.

3.5 Lemma. Let M be an R-module generated by n elements and $\varphi \in \mathrm{End}_R(M)$. If $C \in M_n(R)$ is a matrix associated to φ (with respect to a system of generators $m_1, \ldots, m_n \in M$) and $\chi(x)$ the characteristic polynomial of C then $\chi(\varphi) = 0$.

Proof. By Cayley-Hamilton (3.3), $\chi(C) = 0$, where $\chi = \det(xI - C)$ is the characteristic polynomial of C. Applying the R-algebra homomorphism $\pi \colon R[C] \to R[\varphi]$ mentioned above, we see that $0 = \pi(\chi(C)) = \chi(\varphi)$. □

3.6 Corollary. Let M be an R-module generated by n elements and $\varphi \in \mathrm{End}_R(M)$, such that $\varphi(M) \subseteq JM$ for some ideal $J \trianglelefteq R$. Then φ is a zero of a monic polynomial in $R[x]$ of degree n, $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ with $a_k \in J^{n-k}$ for $0 \leq k < n$.

Proof. If $m_1, \ldots, m_n$ generate M as a R-module and $\varphi(M) \subseteq JM$ then there exist $c_{ij} \in J$ with $\varphi(m_k) = c_{1k} m_1 + c_{2k} m_2 + \ldots + c_{nk} m_n$. Now $\chi(x) = \det(xI - C)$, the characteristic polynomial of $C = (c_{ij})$ is a monic polynomial of degree n with $\chi(\varphi) = 0$ and the property that the coefficient of x^k is in J^{n-k}. □

4. *Integral elements*

4.1 Definition. Let R be a commutative ring, T an R-algebra and $u \in T$. Then u is called **integral** over R if and only if there exists a monic polynomial $f \in R[x]$ with $f(u) = 0$.

4.2 Definition. A ring extension $R \subseteq T$ is called integral if every element of T is integral over R.

4.3 Theorem. Let R be a commutative ring, T an R-algebra and $u \in T$. Then the following are equivalent:

(1) u is integral over R.

(2) $R[u]$ is finitely generated as an R-module.

(3) $R[u] \subseteq A \subseteq T$ for some ring A that is finitely generated as an R-module.

(4) There exists a faithful $R[u]$-module that is finitely generated as an R module.

(5) $R[u]$ is integral over R.

Proof. ($1 \Rightarrow 2$) $R[u]$ is generated as an R-module by the powers of u. Since u is integral over R, there exists an $n \in \mathbb{N}$ and $r_0, \dots, r_{n-1} \in R$ such that $u^n = r_{n-1}u^{n-1} + \ldots + r_1 u + r_0$, and by induction, every power of u is expressible as an R-linear combination of 1, $u, \dots, u^{n-1}$.

($2 \Rightarrow 3$) Take $A = R[u]$.

($3 \Rightarrow 4$) Take A as the faithful $R[u]$ module.

($4 \Rightarrow 5$) Let M be a faithful $R[u]$-module, generated by $m_1, \dots, m_n$ as an R-module, and let $w \in R[u]$. Then $\varphi_w(m) = wm$ (scalar multiplication by w) is an R-module endomorphism of M, $\varphi_w \in \mathrm{End}_R(M)$. Let $C = (c_{ij})$ in $M_n(R)$ be a matrix with with $\varphi_w(m_k) = c_{1k}m_1 + c_{2k}m_2 + \ldots + c_{nk}m_n$ then C represents $\varphi_w \in \mathrm{End}_R(M)$ with respect to the system of generators $m_1, \dots, m_n$.

By Cayley-Hamilton (3.5), $\chi(\varphi_w) = 0$, where $\chi(x) = \det(xI_n - C)$ is the characteristic polynomial of C. $0 = \chi(\varphi_w) = \varphi_{\chi(w)}$, means that scalar multiplication by $\chi(w)$ is the 0-mapping on M, in other words, $\chi(w) \in \mathrm{Ann}_{R[w]}(M)$. Since M is a faithful $R[u]$ module, $\chi(w) = 0$ follows. □

4.4 Definition. Let R be a commutative ring, I an ideal of R, T an R-algebra and $u \in T$. Then u is called **integral** over I if and only if there exists a monic polynomial $f \in R[x]$ whose coefficients (apart from the leading coefficient) are all in I with $f(u) = 0$.

4.5 Theorem. Let R be a commutative ring, I an ideal of R, T an R-algebra and $u \in T$. Then the following are equivalent:

(1) u is integral over I.

(2) $R[u]$ is finitely generated as an R-module and $u \in \sqrt{IR[u]}$.

(3) $R[u] \subseteq A \subseteq T$ for some ring A that is finitely generated as an R-module and $u \in \sqrt{IA}$.

(4) There exists a faithful $R[u]$-module M that is finitely generated as an R module and for some $k \in \mathbb{N}$, $u^k M \subseteq IM$.

Proof. $(1 \Rightarrow 2)$ There exists an $n \in \mathbb{N}$ and $r_0, \ldots, r_{n-1} \in I$ such that $u^n = r_{n-1}u^{n-1} + \ldots + r_1 u + r_0$. Therefore $u \in \sqrt{IR[u]}$ and $R[u]$ is generated as an R-module by $1, u, \ldots, u^{n-1}$.

$(2 \Rightarrow 3)$ Take $A = R[u]$.

$(3 \Rightarrow 4)$ Take A as the faithful $R[u]$ module.

$(4 \Rightarrow 1)$ Let M be a faithful $R[u]$-module, generated by $m_1, \ldots, m_n$ as an R-module. Let $w = u^k$ such that $wM \subseteq IM$. Then $\varphi_w(m) = wm$ (scalar multiplication by w) is an R-module endomorphism of M. Let $C = (c_{ij})$ in $M_n(R)$ be a matrix with with $\varphi_w(m_k) = c_{1k}m_1 + c_{2k}m_2 + \ldots + c_{nk}m_n$ and $c_{ij} \in I$ for all i, j. Then C represents $\varphi_w \in \mathrm{End}_R(M)$ with respect to the system of generators $m_1, \ldots, m_n$.

By Cayley-Hamilton (3.5), $\chi(\varphi_w) = 0$, where $\chi = \det(xI_n - C)$ is the characteristic polynomial of C, whose coefficients (apart from the leading coefficient) are all in I. $0 = \chi(\varphi_w) = \varphi_{\chi(w)}$, means that scalar multiplication by $\chi(w)$ is the 0-mapping on M, in other words, $\chi(w) \in \mathrm{Ann}_{R[w]}(M)$. Since M is a faithful $R[u]$ module, $\chi(w) = 0$ follows. As $w = u^k$ we have also found a monic polynomial satisfied by u whose coefficients (except for the leading coefficient) are in I. □

If $R \subseteq T$ are commutative rings and T is finitely generated as an R-module, then T is also finitely generated over R as a ring, but the converse does not hold in general, viz. the polynomial ring $R[x]$. Integrality provides the answer to the question when the converse does hold. Note the analogy to field extensions, where finitely generated by algebraic elements equals finite-dimensional.

4.6 Proposition. Let R be a commutative ring and T a commutative R-algebra. Then the following are equivalent:

(1) T is finitely generated as an R-module.

(2) T is finitely generated over R a a ring and integral over R.

(3) T is finitely generated by integral elements over R as a ring.

Proof. $(1 \Rightarrow 2)$ by 4.3. $(2 \Rightarrow 3)$ holds a fortiori. To see $(3 \Rightarrow 1)$, assume T is generated as a ring over R by $t_1, \ldots, t_m$. Then T is generated as an R-module by monomials $t_1^{k_1} t_2^{k_2} \ldots t_m^{k_m}$. If each t_i is integral over R then for each i there exists an exponent n_i such that every power of t_i is expressible as an R-linear combination of $1, t, \ldots, t^{n_i}$, and therefore T is generated as an R-module by monomials $t_1^{k_1} t_2^{k_2} \ldots t_m^{k_m}$ with $0 \le k_i \le n_i$. □

4.7 Corollary. Let R be a commutative ring, T an R-algebra and a, $b \in T$ with $ab = ba$. If both $R[a]$ and $R[b]$ are finitely generated as R-modules then so is $R[a, b]$. In particular, if a and b are commuting integral elements over R, then $a - b$ and ab are integral over R, too.

4.8 Corollary. Let $R \subseteq T$ be commutative rings. Then the set of all elements of T integral over R is a ring.

Commutativity is essential here. If the integral elements a and b do not commute, neither their sum nor their product needs to be integral over R.

4.9 Definition. Let $R \subseteq T$ be commutative rings. The ring

$$R' = \{t \in T \mid t \text{ is integral over } R\}$$

is called **the integral closure of R in T**. R is called **integrally closed in T** if $R' = R$. "The" integral closure of a domain R is the integral closure in its quotient field. R is called **integrally closed** if R is integrally closed in its quotient field.

4.10 Proposition. Let R be a commutative ring, $R \subseteq S$ an integral ring extension and u integral over S. Then u is integral over R.

Proof. Suppose $u^n + a_{n-1}u^{n-1} + \ldots + a_0 = 0$ with $a_0, \ldots, a_{n-1} \in S$. Then $R[a_0, \ldots, a_{n-1}]$ is finitely generated integral over R. Let $g_1, \ldots, g_m$ be generators of $R[a_0, \ldots, a_{n-1}]$ as an R-module. Then $R[a_0, \ldots, a_{n-1}, u]$ is generated as an R-module by the elements $g_i u^k$ for $1 \le i \le m$ and $1 \le k \le n-1$. □

4.11 Corollary (Transitivity of integral extensions). Let $R \subseteq S \subseteq T$ be commutative rings. If T is integral over S and S is integral over T then T is integral over R.

4.12 Corollary (Integral closure is integrally closed). Let $R \subseteq T$ be commutative rings and R' the integral closure of R in T. Then R' is integrally closed in T.

4.13 Theorem. Let R be an integrally closed domain with quotient field K, L a field containing K, and $u \in L$ algebraic over K. Then u is integral over R iff the minimal polynomial of u over K is in $R[x]$.

Proof. Assume u integral over R. Let f be the minimal polynomial of u over K and $\bar{L}$ its splitting field over L. Over $\bar{L}$, $f(x) = (x-u)(x-u_1)\dots(x-u_m)$. Since u and the u_i are roots of the same irreducible polynomial on $K[x]$ there exists for each i an isomorphism $\varphi\colon K[u] \to K[u_i]$ with $\varphi(u) = u_i$ and $\varphi(k) = k$ for all $k \in K$. If u is a root of some monic $g \in R[x]$, then $0 = \varphi(0) = \varphi(g(u)) = g(u_i)$ shows u_i to be a root of the same monic $g \in R[x]$. All u_i are integral over R. Therefore the coefficients of f (as sums of products of the roots) are also integral over R. At the same time, the coefficients are in K, therefore, R being integrally closed, the coefficients of f are in R. $\square$

4.14 Lemma. Let $K \subseteq F$ be an algebraic extension of fields and $R \subseteq K$ a domain integrally closed in K.

(i) $u \in F$ is integral over R if and only if its minimal polynomial over K is in $R[x]$.

(ii) Let P be a prime ideal of R. $u \in F$ is integral over P if all coefficients of its minimal polynomial over K (apart from the leading coefficient) are in P.

Proof. Ad (i). Let $f \in K[x]$ be the minimal polynomial of u over K and $g \in R[x]$ with $g(u) = 0$. Then f divides g in $K[x]$. Let $u_1, \dots, u_n$ be the roots of f in its splitting field $\bar{K}$ over F, then all u_i are also roots of g and therefore integral over R. Let R' be the integral closure of R in $\bar{K}$. The coefficients of f (as elementary symmetric polynomials in the u_i are in R'. As they are also in K, they are in $R' \cap K = R$.

Ad (ii). Let f, g as before, and all coefficients (except leading coefficient) of g in P. The roots of f are integral over P, and therefore in $\sqrt{PR'}$. The coefficients of f are, as elementary symmetric polynomials in the u_i, in the subring generated by the u_i in $\bar{K}$, which is contained in $\sqrt{PR'}$. As they are also in K, the coefficients of f are in $K \cap \sqrt{PR'} = \sqrt{P} = P$.

$\square$

4.15 Corollary. Let R be a domain with quotient field K and $u \in L$ algebraic over K. Then u is integral over R iff the coefficients of the minimal polynomial of u over K are integral over R.

4.16 Lemma. Let $R \subseteq T$ be commutative rings and $u \in T$ an invertible element. Then u^{-1} is integral over R if and only if $u^{-1} \in R[u]$.

Proof. An equation showing u^{-1} to be integral over R, such as

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

can be multiplied by u^{n-1} to show u^{-1} to be in $R[u]$:

$$u^{-1} = a_{n-1} + \ldots + a_1 u^{n-2} + a_0 u^{n-1}.$$

Conversely, an equation showing $u^{-1} \in R[u]$, can be multiplied by an appropriate power of u^{-1} to show u^{-1} integral over R. $\square$

4.17 Proposition. Let $R \subseteq L$ be an integral extension of domains. Then R is a field if and only if L is a field.

Proof. If R is a field then L is an algebraic extension of a field and therefore a field. If L is a field and u is a non-zero element of R then u has an inverse u^{-1} in L, which by the previous lemma is in $R[u] = R$. Therefore R is a field. $\square$

4.18 Definition. Ler $R \subseteq T$ be commutative rings. We introduce names for a few properties that the ring extension $R \subseteq T$ may or may not satisfy:

Lying over. For every prime ideal $P \trianglelefteq R$ there exists a prime ideal $\tilde{P} \trianglelefteq T$ with $\tilde{P} \cap R = P$.

Going up. If $P \subseteq Q$ are prime ideals of R and $\tilde{P}$ a prime ideal of T with $\tilde{P} \cap R = P$ then there exists a prime ideal $\tilde{Q}$ of T with $\tilde{P} \subseteq \tilde{Q}$ and $\tilde{Q} \cap R = Q$.

Going down. If $P \subseteq Q$ are prime ideals of R and $\tilde{Q}$ a prime ideal of T with $\tilde{Q} \cap R = Q$ then there exists a prime ideal $\tilde{P}$ of T with $\tilde{P} \subseteq \tilde{Q}$ and $\tilde{P} \cap R = P$.

Incomparability. For any two prime ideals $\tilde{P}$ and $\tilde{Q}$ of T with $\tilde{P} \cap R = \tilde{Q} \cap R$ neither $\tilde{P} \subseteq \tilde{Q}$ nor $\tilde{Q} \subseteq \tilde{P}$ holds.

Let $R \subseteq T$ be commutative rings, P a prime ideal of R and $S = R \setminus P$. If Q is an ideal of T, then $Q \cap R \subseteq P$ if and only if $Q \cap S = \emptyset$. Since S is a multiplicative subset of T containing (0), we know there exist ideals of T not intersecting S, and among them ideals maximal with this property, which are necessarily prime. The question is now whether an ideal maximal among those not intersecting S actually intersects R in P and vice versa. It turns out that the properties “incomparability” and “going up” can be characterized in this way.

4.19 Proposition. Let $R \subseteq T$ be commutative rings. Then the following are equivalent:

(1) $R \subseteq T$ satisfies “going up”.

(2) For every prime ideal P of R, if Q is an ideal of T maximal with respect to the property $Q \cap (R \setminus P) = \emptyset$ then $Q \cap R = P$.

Since ideals maximal with respect to avoiding a multiplicative set S with $0 \notin S$ are guaranteed to exist and are prime, we get:

4.20 Corollary. "Going up" implies "lying over".

4.21 Proposition. Let $R \subseteq T$ be commutative rings. Then the following are equivalent:

(1) $R \subseteq T$ satisfies "incomparability".

(2) For every prime ideal P of R, if Q is a prime ideal of T with $Q \cap R = P$ then Q is maximal with respect to the property $Q \cap (R \setminus P) = \emptyset$.

4.22 Theorem. Let $R \subseteq T$ be an integral extension of rings. Then "incomparability" and "going up" (and therefore "lying over") hold.

Proof. To show "going up", we assume P is a prime ideal of R and $\tilde{P}$ an ideal of T maximal with respect to the property $\tilde{P} \cap (R \setminus P) = \emptyset$; we must show $\tilde{P} \cap R = P$. Suppose otherwise and choose $u \in P \setminus \tilde{P}$. Then, by maximality of $\tilde{P}$, there exists an $s \in (R \setminus P) \cap (\tilde{P} + Tu)$, $s = q + tu$ with $q \in \tilde{P}$ and $t \in T$. t is integral over R, i.e.,

$$t^n + c_{n-1}t^{n-1} + \ldots + c_0 = 0$$

with coeffiecients $c_i \in R$. Multiplying by u^n, we get

$$(tu)^n + c_{n-1}u(tu)^{n-1} + \ldots + u^n c_0 = 0.$$

Since $tu + q = s$, $tu \equiv s \bmod \tilde{P}$, and therefore

$$s^n + c_{n-1}us^{n-1} + \ldots + u^n c_0 \equiv 0 \pmod{\tilde{P}}.$$

The left side of this congruence is in R, so it is actually in $\tilde{P} \cap R \subseteq P$. Since $u \in P$ we get $s^n \in P$ and therefore $s \in P$, a contradiction.

To show "incomparability", we assume $\tilde{P} \cap R = P$ and must show that $\tilde{P}$ is maximal with respect to not intersecting $S = R \setminus P$. Suppose there exists $\tilde{Q}$ with $\tilde{P} \subset \tilde{Q}$ and $\tilde{Q} \cap S = \emptyset$. Choose $u \in \tilde{Q} \setminus \tilde{P}$. u is integral over R. So in particular there exists a monic polynomial f in $R[x]$ with $f(u) \in \tilde{P}$. Let $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ be of minimal degree with this property. Clearly, $\deg f = n \geq 1$. Since $u^n + a_{n-1}u^{n-1} + \ldots + a_0 \in \tilde{P} \subseteq \tilde{Q}$ and $u \in \tilde{Q}$, it follows that $a_0 \in \tilde{Q} \cap R = P$. Now $u(u^{n-1} + a_{n-1}u^{n-2} + \ldots + a_1) \in \tilde{P}$, but no factor is in $\tilde{P}$, a contradiction. $\square$

4.23 Theorem. If $R \subseteq T$ is an integral extension of domains and R is integrally closed then "going down" holds.

Proof. Suppose $P_0 \subseteq P_1$ prime ideals of R and Q_1 a prime ideal of T with $Q_1 \cap R = P_1$. Let $S_0 = R \setminus P_0$, $S_1 = T \setminus Q_1$, and $S = S_0 S_1 = \{rs \mid r \in S_0,\ s \in S_1\}$. S is a multiplicative set containing S_0 and S_1. We will show $P_0 T \cap S =$. Once we have shown this we are done, because then there exists an ideal Q_0 of T maximal with respect to $P_0 T \subseteq Q_0$ and $Q_0 \cap S =$, which is prime, and does what we want.

So, suppose $r \in S_0$ and $s \in S_1$ with $rs \in P_0 T$. Let $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ be the minimal polynomial of rs over K. As rs is integral over P_0, the coefficients $a_0, \ldots, a_{n-1}$ are in P_0. Let

$$g(x) = x^n + \frac{a_{n-1}}{r}x^{n-1} + \frac{a_{n-2}}{r^2}x^{n-2} + \ldots + \frac{a_0}{r^n}$$

then $g(s) = 0$ and g must be the minimal polynomial of s over K (or else we could construct a polynomial in $K[x]$ of degree less than n satisfied by rs). Therefore $b_k = a_k / r^{n-k} \in R$ for $0 \leq k < n$. Now $r^{n-k} b_k = a_k \in P_0$ and $r \notin P_0$ implies $b_k \in P_0$ for $0 \leq k < n$ and s is therefore integral over P_0. So $s \in \sqrt{P_0 T} \subseteq Q_1$, a contradiction. $\square$

The length of a chain of ideals $I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots$ is defined as the number of proper inclusions occurring in the chain.

4.24 Definition. Let P be a prime ideal in a ring R. The **height of** P is the maximal length of a chain of prime ideals descending from P: $\mathrm{ht}(P) = n \in \mathbb{N}_0$ if n is maximal such that there exists a chain of prime ideals $P \supset P_1 \supset \ldots \supset P_n$, and $\mathrm{ht}(P) = \infty$ if there are chains of prime ideals of arbitrary length descending from P.)

4.25 Definition. The **Krull dimension** $\dim(R)$ of a ring R is the supremum of the heights of the prime ideals of R.

Note that a zero-dimensional commutative ring is either a field or else a ring with zero-divisors in which every prime ideal is maximal; and that an integral domain is one-dimensional if and only if every prime ideal other than (0) is maximal.

4.26 Theorem. Let $R \subseteq T$ be commutative rings.

(1) If "incomparability" holds and P is a prime ideal of R then for every prime ideal Q of T with $Q \cap R = P$ we have $\mathrm{ht}(Q) \leq \mathrm{ht}(P)$.

(2) If "going up" holds and P is a prime ideal of R of finite height then there exists a prime ideal Q of R with $Q \cap R = P$ and $\mathrm{ht}(Q) \geq \mathrm{ht}(P)$.

4.27 Corollary. If both "incomparability" and "going up" hold for $R \subseteq T$ (in particular, if $R \subseteq T$ is an integral extension) then for every prime ideal P of R there exists a prime ideal Q of R with $Q \cap R = P$ and $\mathrm{ht}(Q) = \mathrm{ht}(P)$.

Proof. Ad 1) Every chain of prime ideals descending from Q contracts to a chain of the same length descending from P, hence $\mathrm{ht}(P) \geq \mathrm{ht}(Q)$.
Ad 2) "Lying over" and repeated applications of "going up" allow us to construct for every prime ideal chain descending from P a chain of prime ideals in T of the same length descending from some Q with $Q \cap R = P$. □

4.28 Definition. The **co-height** of a prime ideal P of a commutative ring R is the maximal length of a chain of prime ideals ascending from P (in other words, $\text{co-ht}(P) = \dim(R/P)$.)

4.29 Theorem. Let $R \subseteq T$ be commutative rings. If "going up" and "incomparability" hold (in particular, if $R \subseteq T$ is an integral extension) then for every prime ideal P of R and prime ideal Q of T with $Q \cap R = P$ we have $\text{co-ht}(Q) = \text{co-ht}(P)$.

Proof. Easy. □

4.30 Theorem. Let S be a multiplicative subset of a domain R. If R is integrally closed then so is R_S.

Proof. Let K be the quotient field of R and R_S, $u \in K$ integral over R_S; to show $u \in R_S$.

$$u^n + \frac{a_{n-1}}{s_{n-1}} u^{n-1} + \ldots + \frac{a_0}{s_0} = 0 \qquad a_i \in R,\ s_i \in S$$

By multiplication with $s = s_0 \ldots s_{n-1}$ we get

$$su^n + r_{n-1} a_{n-1} u^{n-1} + \ldots + r_0 a_0 = 0 \qquad r_i,\ a_i \in R.$$

Multiplication with s^{n-1} shows su to be integral over R; therefore $su \in R$, and $u \in R_S$. □

4.31 Theorem. Let R_α, $\alpha \in A$ be a collection of integral domains all contained in a field K. If every R_α is integrally closed (in its quotient field) then so is $\bigcap_{\alpha \in A} R_\alpha$. The same holds for "integrally closed in K".

Proof. Easy. □

Since every domain R satisfies $R = \bigcap_{P \text{prime}} R_P = \bigcap_{M \text{maximal}} R_M$, we see:

4.32 Corollary. Let R be an integral domain. Then the following are equivalent:

(1) R is integrally closed.

(2) For every prime ideal P of R, R_P is integrally closed.

(3) For every maximal ideal M of R, R_M is integrally closed.

A commutative ring R is called **normal** if for every prime ideal P of R the localization R_P is an integrally closed domain. We have seen that the concepts of normal and integrally closed coincide in the case of an integral domain.

4.33 Definition. Let R be a commutative ring, T an R-algebra and $u \in T$. Then u is called **almost integral** over R if and only if there exists a finitely generated R-submodule B of T with $R[u] \subseteq B$.

Comparing the definition of "almost integral" with the preceding theorem, we see that

(i) "integral" implies "almost integral"

(ii) for Noetherian R, the notions of "integral" and "almost integral" coincide.

(For Noetherian R, every R-submodule of a finitely generated R-module is finitely generated, such that "almost integral" implies condition (1) of 4.3.)

4.34 Lemma. If R is a domain with quotient field K, then $u \in K$ is almost integral over R if and only if $R[u]$ is a fractional ideal of R, i.e., if there exists a non-zero $d \in R$ such that $dw \in R$ for every $w \in R[u]$, or equivalently, such that $du^n \in R$ for all $n \in \mathbb{N}$:

Proof. If u is almost intgral and $R[u] \subseteq B$, where $b_1, \ldots, b_m$ generate B as an R-module then there exists a non-zero common denominator d with $db_i \in R$ $(1 \leq i \leq m)$ and hence $dR[u] \subseteq dB \subseteq R$. Conversely, if there exists $d \in R$, $d \neq 0$, with $dR[u] \subseteq R$ then $R[u] \subseteq d^{-1}R$, and $d^{-1}R$ is finitely generated (even cyclic) as an R-module. $\square$

4.35 Definition. A domain D with quotient field K is called **completely integrally closed** if every element of K that is almost integral over D lies in D.

As we have seen, for Noetherian domains the notions of "integrally closed" and "completely integrally closed" coincide.

5. *Rings of Quotients and Localization*

A **multiplicatively closed** subset of a ring is a set $S \neq \emptyset$ such that $st \in S$ whenever $s, t \in S$. A multiplicatively closed set S is **saturated**, if S contains all divisors of every $s \in S$. The saturation of a multiplicatively closed set S is $\bar{S} = \{t \in R \mid \exists r \in R \;\; rt \in S\}$.

5.1 Definition. If S is a multiplicatively closed subset of a commutative ring R and $0 \notin S$ then the **ring of fractions of** R **with denominators in** S, $(R_S, +, \cdot)$ and the canonical homomorphism $f_S \colon R \to R_S$ are defined as follows:

R_S is the set of equivalence classes on $S \times R$ under the equivalence relation

$$(s, r) \sim (s', r') \;:\Longleftrightarrow\; \exists t \in S \;\; tsr' = ts'r.$$

The equivalence class of (s, r) is denoted by $\frac{r}{s}$. Addition and multiplication are defined by

$$\frac{r}{s} + \frac{r'}{s'} = \frac{s'r + sr'}{ss'} \qquad \text{and} \qquad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

and the canonical homomorphism $f_S \colon R \to R_S$ by $f_S(r) = \frac{rs}{s}$ (for any $s \in S$).

A lot of facts have to be checked before the above definition can be called valid, for instance that $\sim$ is really an equivalence relation, that addition and multiplication are well-defined (i.e. the resulting equivalence class depends only on the equivalence classes of the arguments and not on the numerator and denominator of the fractions representing them), that R_S satisfies the ring axioms, and that f_S is well-defined and a ring homomorphism. These verifications are easy, if tedious. In doing them, one inevitably encounters the following properties of R_S:

5.2 Remark:

(1) We do not exclude any interesting cases by stipulating $0 \notin S$. If $0 \in S$ then the construction would yield $R_S = \{0\}$.

(2) For all $r \in R$ and $s, t \in S \quad \frac{r}{s} = \frac{rt}{st}$.

(3) R_S is a commutative ring with zero $\frac{0}{s}$ and identity $\frac{s}{s}$ (for any $s \in S$).

(4) $\frac{r}{s} = \frac{r'}{s'}$ iff there exists a $t \in S$ with $trs' = tr's$.

(5) If S contains no zero-divisors, then $\frac{r}{s} = \frac{r'}{s'}$ iff $rs' = r's$.

(6) $\frac{r}{s} = 0$ iff there exists a $t \in S$ with $rt = 0$.

(7) If S contains no zero-divisors, then $\frac{r}{s} = 0$ iff $r = 0$.

(8) $\frac{r}{s}$ is a unit iff there exists a $t \in S$ with $rt \in S$.

(9) If S is saturated, then $\frac{r}{s}$ is a unit iff $r \in S$.

(10) For every $s \in S$ $f_S(s)$ is a unit in R_S.
(11) $\mathrm{Ker} f_S = \{r \in R \mid \exists t \in S\, rt = 0\}$.
(12) f_S is injective iff S contains no zero-divisor.

5.3 Lemma. Let S be a multiplicatively closed subset of R and $\bar{S}$ its saturation. Then $\varphi\colon R_S \to \bar{S}^{-1}R$ given by $\varphi(\frac{r}{s}) = \frac{r}{s}$ is an isomorphism of rings.

Proof. φ is well-defined and a ringhomomorphism; to see injectivity, suppose $\frac{r}{s} \in \mathrm{Ker}\varphi$, then $rt = 0$ for some $t \in \bar{S}$. t divides some $t' \in S$, such that $t'r = 0$ and therefore $\frac{r}{s} = 0$ in R_S. For surjectivity, consider $\frac{r}{t}$ with $r \in R$ and $t \in \bar{S}$. For some $s \in S$ and $w \in R$ we have $s = tw$ (and thus $w \in \bar{S}$) and $\frac{r}{t} = \frac{rw}{tw} = \frac{rw}{s} = \varphi(\frac{rw}{s})$. $\square$

5.4 Proposition. All rings of quotients of R are of the form form R_S with $S = R \setminus \bigcup_{P \in \mathcal{P}} P$ for a set $\mathcal{P}$ of prime ideals of R.

Proof. By the previous lemma, every ring of quotients is of the form R_S with S saturated. By Lemma 10.3, every saturated multiplicative set is the complement of a union of prime ideals and vice versa. $\square$

The importance of the construction lies in the relationship between ideals of R and ideals of R_S. We already know that for every ideal I of R, $f_S(I)R_S$ is an ideal of R_S - the extension of I into R_S. We denote this ideal by I_S.

5.5 Definition. Names and notation for examples of rings of fractions:

- If S is the set of all non-zero-divisors of R, then R_S is called the **total ring of fractions of** R; a special case of this is the **quotient field** of an integral domain, which is R_S with $S = R \setminus \{0\}$.
- If $S = R \setminus P$ for a prime ideal P of R, then R_S is denoted R_P and called the **localization of** R **at** P. The ideal I_S of R_P is denoted I_P or IR_P.

5.6 Remark: The apparent ambiguity of notation in the preceding definition – R_S the ring of fractions with denominators in S, and R_P the ring of fractions with denominators in the complement $R \setminus P$ – we resolve by the following convention: if $0 \notin S$ then R_S denotes the ring of fractions of R with denominators in S, but if $0 \in S$, e.g., if S is a union of prime ideals, then R_S denotes the ring of fractions of R with denominators in $R \setminus S$.

5.7 Lemma. Let I be an ideal of R and $I_S = f_S(I)R_S$ the extension of I to I_S. Then I_S consists of precisely those elements of R_S that admit a representation as a fraction with numerator in I:

$$I_S = \{\frac{i}{s} \in R_S \mid i \in I\}.$$

Proof. ($\subseteq$) is obvious. For ($\supseteq$), let $i \in I$, $s \in S$. Then

$$\frac{i}{s} = \frac{is^2}{s^3} = \frac{is}{s}\frac{s}{s^2} = f_S(i)\frac{s}{s^2} \in f_S(I)R_S.$$

□

Note, however, that $\frac{r}{s} \in I_S$ does not imply $r \in I$, except in special cases such as:

5.8 Lemma. If P is a primary ideal of R with $P \cap S = \emptyset$ then $\frac{r}{s} \in P_S$ implies $r \in P$.

Proof. Let $\frac{r}{s} \in P_S$ with P primary. By 5.7, there exist $p \in P$ and $s' \in S$ with $\frac{r}{s} = \frac{p}{s'}$, and $ts'r = tsp$ for some $t \in S$. Since $ts' \in S$, no power of ts' is in P. Therefore $r \in P$. □

Likewise, for every ideal J of R_S, $f_S^{-1}(J)$ is an ideal of R - the contraction of J to R. (If f_S is injective then $f_S^{-1}(J) = J \cap R$.) Also, if J is a prime [or primary] ideal then so is $f_S^{-1}(J)$.

5.9 Lemma. Let J be an ideal of R_S and I and ideal of R.

The inverse image of J under f_S consists precisely of all numerators that occur in fraction representations of elements of J:

$$f_S^{-1}(J) = \{r \in R \mid \exists s \in S\ \frac{r}{s} \in J\}.$$

Proof. ($\subseteq$) Let $r \in R$ with $f_S(r) \in J$. Then $\frac{s}{s^2} f_S(r) = \frac{s}{s^2}\frac{sr}{s} = \frac{r}{s} \in J$.

For ($\supseteq$), consider $r \in R$ with $\frac{r}{s} \in J$. Then $f_S(r) = \frac{sr}{s} = \frac{r}{s}\frac{s^2}{s} \in J$. □

5.10 Theorem.

(a) For every ideal J of R_S, $(f_S^{-1}(J))_S = J$.

(b) Every ideal of R_S is of the form $I_S = \{\frac{i}{s} \in R_S \mid i \in I\}$ for some ideal I of R.

(c) $I_S = R_S$ iff $I \cap S \neq \emptyset$.

(d) A bijection between those prime ideals P of R with $S \cap P = \emptyset$ and all prime ideals of R_S is given by $P \mapsto P_S$ (for P a prime ideal of R); its inverse is $Q \mapsto f_S^{-1}(Q)$ (for Q a prime ideal of R_S).

(e) Like (d), with “prime” replaced by “primary”.

5.11 Corollary. In terms of extension and contraction by $f_S\colon R \to R_S$, we have $J^{ce} = J$ for every ideal J of R_S and $P^{ec} = P$ for every primary ideal P of R with $P \cap S = \emptyset$.

5.12 Corollary. Let P be a prime ideal of R. Then every ideal of R_P is of the form $I_P = \{\frac{i}{s} \in R_P \mid i \in I\}$ for some ideal I of R with $I \subseteq P$. Via $Q \mapsto Q_P$ the prime ideals of R_P correspond bijectively to the prime ideals Q of R with $Q \subseteq P$. In particular, R_P is a local ring with maximal ideal P_P.

5.13 Definition. A ring containing exactly one maximal ideal is called a **local ring**. (Note, however, that many authors call such rings quasi-local, reserving the name local for Noetherian rings with a unique maximal ideal.)

5.14 Exercise. A ring is local if and only if the set of non-units forms an ideal.

5.15 Theorem (localization commutes with quotients). Let S be a multiplicative subset of R, I an ideal of R, and $\pi\colon R \to R/I$ the canonical projection then

$$(R/I)_{((S+I)/I)} \simeq R_S/I_S.$$

5.16 Easy exercise. The following is a well-defined ring-isomorphism:

$$\frac{(r+I)}{(s+I)} \mapsto \frac{r}{s} + I_S$$

5.17 Corollary. For every prime ideal P of R

$$(R/P)_{(0)} \simeq R_P/P_P.$$

5.18 Definition. If P is a prime ideal of R, we have seen that the quotient field of the integral domain R/P is the same as the residue field of the maximal ideal P_P of R_P. This field is called the **residue field** of P.

*** *Symbolic powers* ***

5.19 Definition. Let P be a prime ideal of R. The n-th symbolic power of P is defined by $P^{(n)} = R \cap P^n R_P$.

The n-th symbolic power of P is the contraction back to R of the extension of P^n into R_P and thus contains P^n.

5.20 Proposition. Let P be a prime ideal of R and $n \in \mathbb{N}$.

(1) $P^{(n)} = (P_P)^n \cap R$

(2) $P^{(n)}$ is P-primary.

(3) If Q is a primary ideal then $P^n \subseteq Q \implies P^{(n)} \subseteq Q$.

(4) $P^{(n)} = P^n \iff P^n$ is primary.

(5) If M is a maximal ideal of R then $M^{(n)} = M^n$ for all $n \in \mathbb{N}$.

Proof. (2) Since P_P is a maximal ideal of R_P, $(P_P)^n$ is P_P-primary. By 10.18, $P^{(n)}$ is P-primary. (4) follows from (2) and (3); (5) follows from (4). $\square$

6. *Valuation rings, Prüfer rings, Dedekind domains.*

6.1 Definition. A commutative ring R is called a valuation ring if for every two elements $a, b \in R$ either $a \mid b$ or $b \mid a$ holds.

The definition of valuation ring is equivalent to saying that the principal ideals of R are totally ordered with respect to inclusion. In fact, more is true.

6.2 Lemma. Let R be a valuation ring. Then the ideals of R are totally ordered with respect to inclusion. In particular, R is a local ring.

Proof. Let I, J be ideals of R and suppose $I \not\subseteq J$. Let $i \in I \setminus J$. Then for all $j \in J$, $j \nmid i$, and therefore $i \mid j$. We have shown $J \subseteq iR \subseteq I$. $\square$

Although the above definition of valuation ring is phrased for commutative rings in general, we will only be interested in valuation rings that are integral domains.

6.3 Remark: Let V be an integral domain contained in a field K. It is easy to see that V is a valuation ring with quotient field K if and only if for every $u \in K$ either $u \in V$ or $u^{-1} \in V$.

6.4 Remark: If V is a valuation ring with quotient field K and R a ring with $V \subseteq R \subseteq K$ then R is also a valuation ring. This is an easy consequence of the preceeding remark.

The unique maximal ideal of a valuation domain V then consists of all elements u in the quotient field K with $u^{-1} \notin V$. Moreover, if M is this unique maximal ideal of V then for every $u \in K$ exactly one of the alternatives $u \in M$ or $u^{-1} \in V$ holds.

$* * *$ *Valuations* $* * *$

6.5 Definition. Let $(G, +)$ be an Abelian group and $\leq$ an order relation compatible with the group operation (i.e., $g \leq g'$ and $h \leq h'$ implies $g + h \leq g' + h'$). Then $(G, +, \leq)$ is called an ordered group. If, moreover, $\leq$ is a total ordering of G (i.e., for all $g, h \in G$, either $g \leq h$ or $h \leq g$ holds) then $(G, +, \leq)$ is called a totally ordered group.

Notation: we will use $g < h$ for "$g \leq h$ and $g \neq h$" and $g \geq h$ for $h \leq g$.

6.6 Definition. Let K be a field and $(G, +)$ a totally ordered group. $v\colon K^* \to G$ (where $K^* = K \setminus \{0\}$) is called a **valuation** on K if

(1) $v(ab) = v(a) + v(b)$ and

(2) $v(a + b) \geq \min(v(a),\, v(b))$.

The subgroup $\Gamma_v = \mathrm{Im}(v)$ of G is called the **valuation group of** v. It is customary to extend the definition of v to all of K by adding an infinity element to G and setting $v(0) = \infty$. With the conventions $\infty + \infty = \infty$, $g + \infty = \infty$ and $g \leq \infty$ for all $g \in G$, (1) and (2) still hold and

(3) $v(a) = \infty \iff a = 0$

Some easy consequences of the definition of a valuation v:

(i) $v(1) = 0$

(ii) $v(a^{-1}) = -v(a)$

(iii) $v(-a) = v(a)$

(iv) $v(a - b) \geq \min(v(a),\, v(b))$

(iv) $v(a) \neq v(b) \implies v(a + b) = \min(v(a),\, v(b))$.

If v is a valuation on K then $R_v = \{k \in K \mid v(k) \geq 0\}$ is a local ring with maximal ideal $M_v = \{k \in K \mid v(k) > 0\}$. (Clearly, the units of R_v are exactly those field elements with both k and k^{-1} in R_v, which are the elements of R_v with $v(k) = 0$.) R_v is a valuation ring, since for all a, $b \in R_v$ either $v(a) \leq v(b)$ or $v(b) \leq v(a)$ and $v(a) \leq v(b)$ means $b/a \in R_v$ and therefore $a \,\big|\, b$ in R_v. We will show that every valuation domain arises from a valuation in this way.

6.7 Lemma. Let R be a valuation domain with quotient field K then the R-submodules of K are totally ordered by inclusion

Proof. Let I, $J \subseteq K$ be R-modules and $I \not\subseteq J$. Let $i \in I \setminus J$. Then for all $j \neq 0$ in J either $i/j \in R$ or $j/i \in R$, but $i/j \in R$ is impossible, since it would imply $i = j(i/j) \in J$. Therefore for all $j \neq 0$ in J we have $j/i \in R$, which implies $j = i(j/i) \in iR \subseteq I$. Thus $I \not\subseteq J$ implies $J \subseteq iR \subseteq I$. □

6.8 Proposition. Let R be a valuation domain with quotient field K. Then $G = \{zR \mid z \in K,\, z \neq 0\}$ is totally ordered by

$$yR \leq zR \iff yR \supseteq zR$$

and

$$yR \star zR := yzR$$

defines an Abelian group structure on G compatible with the ordering. Moreover,

$$v\colon K^* \to G \qquad v(z) = zR$$

is a valuation on K with $R = \{k \in K \mid v(k) \geq 0\}$.

Proof. Easy. $\square$

$* * *$ *Valuation rings and integral closure* $* * *$

6.9 Definition. A ring is called **Bézout ring** if every finitely generated ideal is principal.

6.10 Remark: It is clear that every valuation ring is a Bézout ring. In particular, every valuation ring is a GCD-ring. Therefore every valuation domain is integrally closed. (This is of course easy to show directly.)

We have seen that valuation domains are integrally closed. It follows that arbitrary intersections of valuation domains contained in a field are integrally closed. We shall see that conversely, every integral closure of a domain is an intersection of valuation domains.

Before showing this, however, we note in passing that valuation rings are characterized among local rings by the Bézout ring property.

6.11 Lemma. A local ring is a valuation ring if and only if it is a Bézout ring.

Proof. Every valuation ring is a Bézout ring. Conversely, let R be a local Bézout ring and a, $b \in R$. We must show $a \mid b$ or $b \mid a$. By dividing a and b by their greatest common divisor, we may assume $\gcd(a, b) = 1$ and therefore $Ra + Rb = R$. This shows that a and b are not both in the unique maximal ideal of R, hence one of them is a unit and therefore divides the other. $\square$

6.12 Lemma. Let $R \subseteq T$ be commutative rings, I an ideal of R and $u \in T$ a unit. If $IR \neq R$ then $IA \neq A$ for either $A = R[u]$ or for $A = R[u^{-1}]$.

Proof. Suppose otherwise. Then there exist a_i and $b_i \in I$ such that

$$(*) \qquad 1 = a_0 + a_1 u + \ldots + a_n u^n$$

$$(**) \qquad 1 = b_0 + b_1 u^{-1} + \ldots + b_m u^{-m}$$

where n, $m \in \mathbb{N}$ are minimal and w.l.o.g. $n \geq m$.

Multiplication of $(**)$ with u^n gives

$$(1 - b_0)u^n = -b_1 u^{n-1} - \ldots - b_m u^{n-m}.$$

By multiplying $(*)$ with $(1 - b_0)$ and substituting for $(1 - b_0)u^n$ from the above formula we can express 1 as an I-linear combination of powers u^k with $0 \leq k \leq n-1$, contradicting the minimality of n. $\square$

6.13 Lemma. Let $R \subseteq K$ be an integral domain contained in a field and I an ideal of R. If $I \neq R$ then there exists a valuation domain V with quotient field K such that $R \subseteq V$ and $IV \neq V$.

Proof. Let $\mathcal{S}$ be the set of pairs (R_α, I_α) where R_α is a ring with ideal $I_\alpha \neq R_\alpha$ and $R \subseteq R_\alpha$ as well as $I \subseteq I_\alpha$. We order $\mathcal{S}$ by $(R_\alpha, I_\alpha) \leq (R_\beta, I_\beta)$ if and only if both $R_\alpha \subseteq R_\beta$ and $I_\alpha \subseteq I_\beta$. By Zorn's Lemma, $\mathcal{S}$ has a maximal element (V, J). We know $IV \neq V$, since $I \subseteq J$. Now let u be an element of K, we must show $u \in V$ or $u^{-1} \in V$. Suppose not. Since by a previous lemma the extension of J is a proper ideal of either $V[u]$ or $V[u^{-1}]$, either $(V[u], JV[u])$ or $(V[u^{-1}], JV[u^{-1}])$ is an element of $\mathcal{S}$ strictly greater than (V, J), a contradiction. $\square$

6.14 Theorem. Let R be an integral domain with quotient field K and R' the integral closure of R. Then $R' = \bigcap_{R \subseteq V \subseteq K} V$, where V ranges over all valuation domains between R and K.

Proof. $\bigcap_{R \subseteq V \subseteq K} V$ contains R, is integrally closed (as an intersection of integrally closed domains) and therefore contains R'. Conversely, let $z \in \bigcap_{R \subseteq V \subseteq K} V$; we must show z is integral over R. Suppose not. Let $z = u^{-1}$. Then $u^{-1} \notin R'$ implies $u^{-1} \notin R[u]$. Since u is not a unit in $R[u]$, $uR[u] \neq R[u]$ and there exists a valuation domain V containing $R[u]$ with $uV \neq V$. This contradicts $z = u^{-1} \in V$. $\square$

$* * *$ *Invertible ideals and Prüfer rings* $* * *$

6.15 Definition. Let R be an integral domain with quotient field K and I an R-submodule of K.

- I is called a **fractional ideal** of R if there exists a non-zero $r \in R$ such that $rI \subseteq R$.
- The inverse of I is defined as $I^{-1} = \{z \in K \mid zI \subseteq R\}$.
- I is called invertible if $I^{-1}I = R$. (Note that $I^{-1}I \subseteq R$ is automatic.)

In the context of invertible ideals, fractional ideals are usually just called ideals, "fractional" being understood. No confusion should result.

6.16 Remark:

1) Every finitely generated R-submodule of K is a fractional ideal. (We can multiply I by a common denominator of the generators.)

2) Every non-zero principal fractional ideal is invertible. (The inverse of Ra is Ra^{-1} and $RaRa^{-1} = R$.)

6.17 Proposition. Let I be an R-submodule of K. If I is invertible then I is finitely generated.

Proof. $I^{-1}I = R$, so there exist $a_i \in I^{-1}$ and $b_i \in I$ with $\sum_{i-1}^{n} a_i b_i = 1$. We claim the b_i generate I. Let $c \in I$. $c = 1c = \sum_{i-1}^{n} a_i c b_i =$. Now $a_i \in I^{-1}$ implies $a_i c \in R$ and we have $c = \sum_{i-1}^{n} r_i b_i$ with $r_i \in R$. $\square$

6.18 Definition. A commutative ring R with only finitely many maximal ideals is called **semi-local.**

6.19 Proposition. Let R be a semi-local domain. Then every invertible ideal is principal.

Proof. Let $M_1, \ldots, M_n$ be the maximal ideals of R. By $II^{-1} = R$, there exist $a_i \in I$ and $b_i \in I^{-1}$ such that $a_i b_i \notin M_i$. By the Chinese Remainder Theorem, there exists $u_i \in R$ with $u_i \notin M_i$ and $u_i \in \bigcap_{j \neq i} M_j$. Let $v = \sum_{i=1}^{n} u_i b_i$. Then $vI \subseteq R$ is an ideal of R and not contained in any M_i, since $va_i \notin M_i$. Therefore $vI = R$. This shows $I = v^{-1}R$. I is principal. $\square$

To be able to consider localizations of fractional ideals we need to extend the construction of rings of fractions to modules:

6.20 Definition. Let R be a commutative ring, $S \subseteq R$ a multiplicative set and M an R-module. The R_S-module M_S is defined as follows: Its elements are the equivalence classes on $S \times M$ w.r.t. the equivalence relation

$$(s, m) \sim (s', m') \;:\Longleftrightarrow\; \exists t \in S \; t(sm' - s'm) = 0.$$

The equivalence class of (s, m) is denoted by $\frac{m}{s}$. Addition and scalar multiplication are defined by:

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \qquad \text{and} \qquad \frac{r}{s} \cdot \frac{m}{s'} = \frac{rm}{ss'}$$

If $S = R \setminus P$ for a prime ideal P of R then M_S is denoted M_P and called the localization of M at P.

6.21 Remark:

(i) The zero-element of M_S is $\frac{0}{s}$ for any $s \in S$, and $\frac{m}{s} = 0$ iff there exists a $t \in S$ with $tm = 0$.

(ii) The map $f\colon M \to M_S$ given by $f(m) = \frac{sm}{s}$ (or $f(m) = \frac{m}{1}$, if $1 \in S$) is an R-module homomorphism with $\mathrm{Ker} f = \{m \in M \mid \exists s \in S \; sm = 0\}$.

6.22 Lemma. If $f\colon M \to N$ is an R-module homomorphism, then

$$f_S\colon M_S \to N_S \qquad f_S(\frac{m}{s}) := \frac{f(m)}{s}$$

is an R_S-module homomorphism. Also,

(i) $S^{-1}\mathrm{id}_M = \mathrm{id}_{M_S}$

(ii) $f_S \circ g_S = S^{-1}(f \circ g)$

(iii) $\mathrm{Ker} f_S = S^{-1}\mathrm{Ker} f$; $\quad \mathrm{Im} f_S = S^{-1}\mathrm{Im} f$

(Furthermore, S^{-1} is an exact functor, i.e. it maps exact sequences of R-modules to exact sequences of R_S-modules.)

6.23 Proposition. Let I be an invertible ideal of a domain R, $S \subseteq R$ a multiplicative subset of R. Then I_S is an invertible ideal of R_S.

Proof. Easy. □

6.24 Theorem. Let I be a finitely generated ideal of an integral domain R. Then I is invertible if and only if I_M is principal for every maximal ideal M of R.

Proof. If I is invertible, we have seen that I_M is invertible and hence principal for every maximal ideal M of R. Conversely, assume every I_M is principal. Suppose I is not invertible then $II^{-1} \subseteq M$ for some maximal ideal M of R. I_M is principal, and we may choose a generator in I: $I_M = iR_M$, with $i \in I$. Let $I = Ri_1 + \ldots + Ri_n$. Then there exist $r_k \in R$ and $s_k \in R \setminus M$ with $i_k = \frac{r_k}{s_k} i$. Set $s = s_1 \ldots s_n$. Then $si^{-1}i_k \in R$ for every generator i_k of I, and therefore $si^{-1} \in I^{-1}$. This implies $s = si^{-1}i \in I^{-1}I \subseteq M$, a contradiction to $s \in R \setminus M$. □

6.25 Theorem. Let R be an integral domain. Then the following are equivalent.

(1) Every finitely generated non-zero ideal of R is invertible.

(2) R_P is a valuation domain for every prime ideal P of R.

(3) R_M is a valuation domain for every maximal ideal M of R.

6.26 Definition. A domain satisfying one (and hence all) of the equivalent conditions in the preceding theorem is called Prüfer domain.

Proof. ($1 \Rightarrow 2$) We show that R_P is Bézout. Let $\frac{r_1}{s_1}, \ldots, \frac{r_n}{s_n} \in R_P$, $r_i \in R$, $s_i \in R \setminus P$. Since R is Prüfer, $I = r_1R + \ldots r_nR$ is invertible, and therefore $I_P = \frac{r_1}{s_1}R_P + \ldots + \frac{r_n}{s_n}R_P$ is invertible. Since R_P is local, invertible implies principal.
($2 \Rightarrow 3$) Obvious.
($3 \Rightarrow 1$) If I is a finitely generated ideal of R then I_M is principal (as a finitely generated ideal in the Bézout domain R_M) for all maximal ideals M of R. Therefore I is invertible. □

6.27 Theorem. Let R be a Prüfer domain with quotient field K. If V is a valuation ring with $R \subseteq V \subseteq K$ then $V = R_P$ for some prime ideal P of R.

Proof. Let M be the maximal ideal of V and $P = M \cap R$. For any $s \in R \setminus P$, $s \notin M$ implies $s^{-1} \in V$. Therefore $R_P \subseteq V$.

Suppose $V \not\subseteq R_P$. Let $v \in V \setminus R_P$. Since R_P is a valuation domain, $v^{-1} \in R_P$. This means $v = \frac{s}{r}$ with $r \in R$, $s \in R \setminus P$. We must have $r \in P$, since otherwise $v \in R_P$. Now $s = rv \in PV \subseteq M$, a contradiction. □

$* * *$ *Discrete valuation rings and Dedekind domains* $* * *$

6.28 Theorem. Let R be a local integral domain with maximal ideal M, and not a field. The following are equivalent:

(1) R is Noetherian and integrally closed and $\dim R = 1$.

(2) R is Noetherian and M is principal.

(3) R is a unique factorization domain with just one (up to units) irreducible element.

(4) R is a principal ideal domain.

Proof. $(1 \Rightarrow 2)$ Let $m \in M$ with $m \neq 0$ and $mR \neq M$ and consider the ring $T = R/mR$. mR not being prime, T is not a domain. The set $\mathcal{Z}(T)$ of zero-divisors of T is a union of prime ideals by 10.4, therefore $\mathcal{Z}(T)$ equals the unique prime ideal of T: $\mathcal{Z}(T) = M/mR$. By 8.7 (universal zero-divisor) applied to the ideal M/mR of T, there exists $a \in R \setminus mR$ such that $aM \subseteq mR$.

Now $\frac{a}{m} \in M^{-1} \setminus R$ and $\frac{a}{m}M$ is an ideal of R. Suppose $\frac{a}{m}M \neq R$. Then $\frac{a}{m}M \subseteq M$ and therfore $R[\frac{a}{m}]M \subseteq M$. Now M is a faithful $R[\frac{a}{m}]$-module and finitely generated as an R-module, which means $\frac{a}{m}$ is integral over R and therefore in R; a contradiction. Therefore $\frac{a}{m}M = R$ and $M = \frac{m}{a}R$ is principal.

$(2 \Rightarrow 3)$ The ascending chain condition implies that every non-zero element is a product of irreducible elements (the ascending chain condition for principal ideals suffices for that). Also, every irreducible element is prime, and there is (up to multiplication by units) only one irreducible element. (Since the unique maximal ideal M of R is principal, it is the only principal ideal maximal among proper principal ideals, and therefore the only ideal generated by an irreducible ideal. So there is up to multiplication by units only one irreducible element and it generates M. Now M is also a prime ideal, wherfore the unique (up to units) irreducible element is also prime). Together this implies a unique factorization domain with just one irreducible element.

$(3 \Rightarrow 4)$ and $(4 \Rightarrow 1)$ are easy. □

6.29 Definition. A domain satisfying one (and hence all) of the equivalent conditions in the preceeding theorem is called **discrete valuation domain (DVR)**, or, more precisely **discrete valuation domain of rank 1**.

6.30 Proposition. A domain is a DVR if and only if it is the valuation ring of a valuation with value group isomorphic to $(\mathbb{Z}, +)$.

Proof. Exercise. $\square$

6.31 Theorem. Let R be an integral domain. Then the following are equivalent

(1) Every non-zero ideal of R is invertible.

(2) R is Noetherian and integrally closed and $\dim R \leq 1$.

(3) R is either a field or a Noetherian domain s.t. for every maximal ideal M of R, R_M is a DVR.

6.32 Definition. A domain satisfying one (and hence all) of the equivalent conditions in the preceding theorem is called a **Dedekind ring**.

Proof. $(1 \Rightarrow 3)$ Invertible implies finitely generated, so R is Noetherian. Let M be a maximal ideal of R. Every ideal of R_M is of the form I_M for an invertible ideal I of R and hence is principal. R_M is a local principal ideal domain and therefore a DVR.

$(3 \Rightarrow 1)$ For every non-zero ideal I of R, every localization I_M at a maximal ideal is principal, since R_M is a principal ideal domain.

$(3 \Rightarrow 2)$ R is integrally closed as the intersection of its localizations R_M, which are integrally closed as valuations rings. The Krull dimension of R is the supremum of $\dim R_M$, where M ranges through the maximal ideals of R and therefore $\dim R \leq 1$.

$(2 \Rightarrow 3)$ If $\dim R \leq 1$ and R is not a field, then $\dim(R) = 1$. For every maximal ideal M of R, the localization R_M is local, Noetherian, integrally closed and one-dimensional and therefore a DVR by the previous Theorem. $\square$

6.33 Theorem. Let D be a domain. If every non-zero ideal of D is invertible, then every non-zero ideal is expressible as a product of prime ideals.

Proof. Invertible implies finitely generated, so D is Noetherian. Suppose there exist non-zero ideals not expressible as products of prime ideals. The set of such ideals has a maximal element, I. This I is not R (since R is an empty product of prime ideals); nor is I itself prime, so there exists a prime ideal $P \supset I$ properly containing I. We have $I \subseteq IP^{-1} \subseteq R$. If $IP^{-1} = I$, then (since P is invertible) multiplication by P gives $I = IP$ and by Nakayama's Lemma, there is an element $a \in R$ with $aI = 0$ and $a \equiv 1 \bmod P$, which is impossible in a domain. Therefore IP^{-1} properly contains I and, by maximality of I, is expressible as a product of prime ideals $IP^{-1} = P_1 \ldots P_m$. Using $PP^{-1} = R$ again, we get $I = P_1 \ldots P_m P$, a contradiction. $\square$

6.34 Corollary. In a Dedekind ring, every non-zero ideal is uniquely expressible as a product of prime ideals.

Proof. By 6.31, every non-zero ideal in a Dedekind ring is invertible, so 6.33 implies existence of a factorization. If $P_1 \ldots P_n = Q_1 \ldots Q_m$ then P_1, being prime, contains one of the Q_i, say $Q_1 \subseteq P_1$. Since D is at most 1-dimensional, it follows that $Q_1 = P_1$ and we can cancel invertible ideals and get $P_2 \ldots P_n = Q_2 \ldots Q_m$. Inductively we see that the factorizations are the same (up to order). $\square$

6.35 Remark: Prime factorization of ideals characterizes Dedekind rings, even without the assumption of uniqueness: a domain in which every ideal is a product of prime ideals is a Dedekind domain.

$* * *$ *rank 1 valuation rings* $* * *$

6.36 Definition. An ordered group $(\Gamma, +)$ satisfies the **Archimedean axiom** if for any a, $b \in \Gamma$ with $a > 0$ there exists $n \in \mathbb{N}$ with $na \geq b$.

6.37 Proposition. An ordered group satisfies the Archimedean axiom if and only if it is order-isomorphic to a subgroup of $(\mathbb{R}, +)$.

Proof. Every subgroup of $(\mathbb{R}, +)$ satisfies the Archimedean axiom. Now let $(\Gamma, +)$ be an ordered group satisfying the Archimedean axiom and fix an element $a > 0$ of Γ. We will construct an order-preserving injective map $f \colon \Gamma \to \mathbb{R}$ by defining a Dedekind cut for every $b \in \Gamma$. First consider only elements $b > 0$ and define

$$S_b = \{\frac{m}{n} \in \mathbb{Q} \mid m \in \mathbb{Z}, n \in \mathbb{N},\ ma \leq nb\}.$$

Note that $\frac{m}{n} \in S_b$ and $\frac{\tilde{m}}{\tilde{n}} = \frac{m}{n}$ (with n, $\tilde{n} > 0$) implies that $\tilde{m}a \leq \tilde{n}b$. Also, by the Archimedean axiom, $S_b \neq \mathbb{Q}$ and $S_b \neq \emptyset$.

If $\frac{m}{n} \in S_b$ then every $\frac{m'}{n'} \leq \frac{m}{n}$ in $\mathbb{Q}$ is also in S_b. (By choosing a common denominator, we may assume $n' = n$, which implies $m' \leq m$, and then $m'a \leq ma \leq nb = n'b$.) S_b thus defines a unique real number $\sup S_b$ and we set $f(b) = \sup S_b$. We extend the definition of f to all of Γ by seting $f(0) = 0$ and $f(b) = -f(-b)$ for $b < 0$. It is then not hard to check that f is an order-preserving group homomorphism and injective. $\square$

6.38 Proposition. Let v be a valuation on a field K with valuation ring R_v and valuation group $\Gamma_v \neq 0$. Then Γ_v satisfies the Archimedean axiom if and only if $\dim R_v = 1$.

Proof. Assume the Archimedean axiom. $\Gamma_v \neq 0$ implies that R_v is not a field. Suppose $\dim R > 1$. Then there exists a prime ideal P with $(0) \subset P \subset M_v$. Let $a \in M_v \setminus P$ and $b \in P \setminus (0)$ and set $\alpha = v(a)$, $\beta = v(b)$. Since $\alpha > 0$ there exists $n \in \mathbb{N}$ with $n\alpha \geq \beta$. This means $v(a^n) \geq v(b)$, i.e., $\frac{a^n}{b} \in R_v$ and therfore $a^n \in bR_v \subseteq P$. We conclude that $a \in P$, a contradiction.

Conversely, assume $\dim R = 1$. R is a one-dimensional local ring, so M_v is its only non-zero prime ideal and therefore the radical of every proper non-zero ideal. In particular, for every non-zero $a \in M_v$ and any $b \in R_v$ there exists $n \in \mathbb{N}$ such that $a^n \in bR_v$, which implies that for every $\alpha > 0$ in Γ and every $\beta \geq 0$ in Γ there exists $n \in \mathbb{N}$ with $n\alpha = \gamma + \beta$ for some $\gamma \geq 0$, or in other words, $n\alpha \geq \beta$. □

$* * *$ *Quick and dirty Dedekind ring properties* $* * *$

6.39 Lemma. In a Noetherian ring, every non-zero ideal contains a product of non-zero prime ideals.

Proof. Suppose M maximal among the counterexamples. Then M is not prime, so there exist r, s with $rs \in M$ but $r \notin$M and $s \notin M$. Since M is striclty contained in $M + rR$ and $M + sR$, these ideals each contain a product of prime ideals, and so does $(M + rR)(M + sR)$, which is contained in M, a contradiction. □

6.40 Lemma. Let R be a Noetherian ring with $\dim R = 1$ and quotient field K, and $(0) \subsetneqq I \subsetneqq R$ a proper ideal of R. Then there exists $\gamma \in K \setminus R$ with $\gamma I \subseteq R$.

Proof. Let $a \neq 0$ in I then there exist non-zero prime ideals $P, P_1, \ldots, P_r$ with $P \supseteq I \supseteq aR \supseteq P_1 \cdot \ldots \cdot P_r$, where r is minimal with the property that aR contains a product of r prime ideals. P being prime, it contains one of the P_i, say $P_1 \subseteq P$ and therefore $P_1 = P$. So we have

$$P \supseteq I \supseteq aR \supseteq P \cdot P_2 \cdot \ldots \cdot P_r.$$

Pick $b \in P_2 \cdot \ldots \cdot P_r \setminus aR$ (possible by minimality of r) and set $\gamma = b/a$. Then $\gamma \notin R$, and for every $i \in I$, $i\gamma = (ib)/a$ is in R, because $ib \in P \cdot P_2 \cdot \ldots \cdot P_r \subseteq aR$.
□

6.41 Theorem. In a Dedekind ring, every non-zero ideal is invertible.

Proof. Let $I \neq (0)$ and suppose $I^{-1}I \subsetneqq R$. Let $\gamma \in K \setminus R$ with $\gamma I^{-1}I \subseteq R$, then $\gamma I^{-1} \subseteq I^{-1}$. This makes I^{-1} a faithful $R[\gamma]$-module which is finitely generated as R-module, showing $\gamma \in K \setminus R$ to be integral over R - a contradiction to R being integrally closed. $\square$

6.42 Corollary. In a Dedekind ring, every non-zero ideal is a product of prime ideals, and this prime factorization is unique.

Proof. Existence first: R is an empty product of prime ideals. Let $I \neq R$ be a non-zero ideal of R then $I \subseteq P_0$ for some prime ideal P_0. If $I = P_0$ we are done. If $I \subset P_0$, then, P_0 being invertible, $I = (IP_0^{-1})P_0$ and we can iterate the process of finding a prime factor with $I_1 = (IP_0^{-1})$. This process terminates with $I_n = IP_0^{-1} \ldots P_{n-1}^{-1} = P_n$ a prime ideal (and therefore $I = P_0^{-1} \ldots P_n$) because otherwise we would have an infinte ascending chain of ideals $I \subset I_1 \subset I_2 \subset \ldots$, where $I_k = IP_0^{-1} \ldots P_{k-1}$.

Uniqueness: Suppose $P_1 \ldots P_n = Q_1 \ldots Q_m$, all P_i and Q_i prime. Induction on $\min(n, m)$. If $P_1 \ldots P_n = Q_1$ then, Q_1 being prime, there exists an index i with $P_i \subseteq Q_1$, w.l.o.g. $P_1 \subseteq Q_1$. As P_1 is maximal, we have $P_1 = Q_1$. We see that $n = 1$, because multiplication with P_1^{-1} gives $P_2 \ldots \mathcal{P}_n = R$, in particular $R \subseteq P_i$ for $i \geq 2$, therefore prime ideals with indices $i \geq 2$ do not exist.

If $\min(n, m) > 1$ and $P_1 \ldots P_n = Q_1 \ldots Q_m$, then again $P_1 \ldots P_n \subseteq Q_1$ implies that for some i $P_i = Q_1$, w.l.o.g. $P_1 = Q_1$, and we may cancel $P_1 = Q_1$ by multiplying both sides with Q_1^{-1}, and get $P_2 \ldots P_n = Q_2 \ldots Q_m$. By induction hypothesis $n = m$ and $P_2, \ldots, P_n$ and $Q_2, \ldots, Q_n$ are (up to order) the same list of prime ideals. $\square$

7. *Noetherian Rings.*

7.1 Proposition. Let R be a commutative ring. Then the following are equivalent:

(1) Every ideal of R is finitely generated.

(2) Every ascending chain of ideals of R is of finite length.

(3) Every non-empty set of ideals of R has a maximal element.

Proof. $(1 \Rightarrow 2)$ and $(2 \Rightarrow 3)$ are easy.
$(3 \Rightarrow 1)$ Let I be an ideal of R and $\mathcal{S}$ the set of finitely generated ideals contained in I. $\mathcal{S}$ (being non-empty because it contains (0)) has a maximal element J. Suppose $J \neq I$ and pick $i \in I \setminus J$. Then $iR + J \subseteq I$ is finitely generated and strictly contains J, a contradiction. $\square$

7.2 Definition. A commutative ring satisfying one and hence all of the equivalent conditions of the preceeding theorem is called Noetherian.

Condition (2) above is called "the ascending chain condition" (ACC) (for ideals). Similar conditions for objects other than ideals, or for special kinds of ideals, often play a rôle. For instance, a generalization of Noetherian domains is given by requiring the ascending chain condition only for divisorial ideals; the resulting domains are called Mori domains.

7.3 Definition. Let R be a commutative ring, M an R-module. M is called **Noetherian** if every R submodule of M is finitely generated.

Since the ideals of a ring R are precisely the R-submodules of R, a ring R is Noetherian (as a ring) if and only if it is a Noetherian R-module.

7.4 Remark: As in Proposition 7.1, the following are equivalent:

(1) M is a Noetherian R-module

(2) Every ascending chain of R-submodules of M is of finite length.

(3) Every non-empty set of R-submodules of M contains a maximal element.

7.5 Lemma. Let M be am R-module and L a submodule of M. Then M is Noetherian if and only if both L and M/L are Noetherian.

Proof. If M is Noetherian, then L is Noetherian, since every submodule of L is s submodule of M. Also, M/L is Noetherian, since every submodule of M/L is of the form $\pi(N)$, where N is a submodule of M and $\pi\colon M \to M/L$ the canonical projection, and $\pi(N)$ is generated by the images under π of a set of generators of N.

Conversely, suppose L and M/L are Noetherian. Given a submodule N of M, let a $n_1,\dots n_s$ be generators of $N \cap L$ and $m_1 + L,\dots,m_t + L$ generators of $(N + L)/L$ with $m_1,\dots,m_t \in N$. Then N is generated by $n_1,\dots n_s, m_1,\dots,m_t$. □

7.6 Proposition. For every Noetherian ring R, every finitely generated R-module is Noetherian.

Proof. We only need to show that every free R-module of finite rank is Noetherian, since every R-module generated by n elements is a homomorphic image of the free R-module of rank n.

Induction on the rank of M: For $n = 1$, $M = R$, and R is Noetherian. For $\operatorname{rank}(M) = n > 1$, $M = R \oplus L$, L a free R-module of rank $n - 1$. L is Noetherian by induction hypothesis, $M/L = R$ is Noetherian, and therefore M is Noetherian by the previous Lemma. □

7.7 Theorem (Hilbert's basis theorem). Let R be a Noetherian ring. Then $R[x]$ is Noetherian.

Proof. Let $J \neq (0)$ be an ideal of $R[x]$. For $n \in \mathbb{N}$, let I_n be the set of leading coefficients of polynomials of degree n or less in J and set $I = \bigcup_{n\in\mathbb{N}} I_n$. The I_n are ideals of R with $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ and therfore I is an ideal of R too. The fact that both I and all I_n are finitely generated now implies that J is finitely generated: let $g_1,\dots,g_m \in J$ be polynomials whose leading coefficients generate I and let $N = \max_{1\le k\le m} \deg g_k$. To $g_1,\dots,g_m$ we add for each $n < N$ a finite set of elements of J of degree n or less whose leading coefficients generate I_n. That the resulting finite set of polynomials generates J is now easily seen by induction on the degree of an element of J. □

7.8 Corollary. Let R be a Noetherian ring. Then $R[x_1,\dots,x_n]$ and therefore every finitely generated R-algebra (as a homomorphic image of a polynomial ring $R[x_1,\dots,x_n]$) is Noetherian.

7.9 Lemma. Let R be a commutative ring and P an ideal of R that is not finitely generated and which is maximal with respect to this property. Then P is prime.

Proof. Suppose $ab \in P$ and $a \notin P$, $b \notin P$. By maximality of P, $P + (a)$ is finitely generated, by elements $p_1 + r_1 a$, …, $p_k + r_k a$ (with $p_i \in P$, $r_i \in R$), and similarly,

$P+(b)$ is finitely generated, by elements $q_1+s_1b,\ \ldots,\ q_m+s_mb$ (with $q_i\in P$, $s_i\in R$).

Also, the ideal $(P:a)=\{r\in R\mid ra\in P\}$ properly containes P (because $P\subset P+(b)\subseteq(P:a)$), and is therefore finitely generated, by $j_1,\ldots,j_h$, say.

If $c\in P$, then $c\in P+(a)$ and there exist $t_1,\ldots,t_k\in R$ with $c=t_1p_1+\ldots+t_kp_k+(t_1r_1+\ldots+t_kr_k)a$. Let $d=t_1r_1+\ldots+t_kr_k$, then $da=c-(t_1p_1+\ldots+t_kp_k)\in P$ and therefore $d\in(P:a)$. Let $t_1',\ldots,t_h'\in R$ such that $d=t_1'j_1+\ldots+t_h'j_h$.

Then $c=t_1p_1+\ldots+t_kp_k+t_1'j_1a+\ldots+t_h'j_ha$, and $p_1,\ldots,p_k$ as well as $j_1a,\ldots,j_ha$ are in P. We have shown that $p_1,\ldots,p_k,j_1a,\ldots,j_ha$ generate P, a contradiction. $\square$

7.10 Theorem (Cohen). Let R be a commutative ring. If every prime ideal of R is finitley generated, then R is Noetherian.

Proof. The set of non-finitely-generated ideals of a commutative ring clearly satisfies the hypothesis of Zorn's lemma. Therefore, if this set is non-empty, it has a maximal element by Zorn's lemma. Such a maximal element is a prime ideal by the previous lemma. Therefore, every non-Noetherian ring has a prime ideal that is not finitely generated. $\square$

∗∗∗ *Zero-divisors and associated primes* ∗∗∗

The following theorem holds for (not necessarily Noetherian) commutative rings:

8.1 Theorem (Prime Avoidance). Let R be a commutative ring and $P_1, \dots, P_n$ ideals of R such that at most two of the P_i are not prime. Let I be a ring (possibly without a unit element) such that $I \subseteq \bigcup_{1 \le i \le n} P_i$. Then there exists an i with $S \subseteq P_i$.

Proof. Induction on n. Let $n=2$, $I \subseteq P_1 \cup P_2$, and suppose there exists $a_1 \in S \subseteq P_1$ and $a_2 \in S \subseteq P_2$. Then $a_1 + a_2$ is in I, but neither in P_1 nor in P_2, a contradition. Now let $n > 2$, $I \subseteq \bigcup_{1 \le i \le n} P_i$, but for every $1 \le k \le n$, I is not contained in the union of the P_i with $i \ne k$ (otherwise we are done by induction hypothesis). For every k pick a_k in I and not in the union of the P_i with $i \ne k$. Then $a_k \in P_k$. As $n > 2$, at least one of the P_i is prime, say P_1 is prime, and we set $b = a_1 + a_2 \dots a_n$. Then b is in I, but not in any P_i, a contradiction □

8.2 Definition. Let M be an R-module.

(i) For $m \in M$, the **annihilator** of m is $\mathrm{Ann}_R(m) := \{r \in R \mid rm = 0\}$.

(ii) $r \in R$ is a **zero-divisor** of M if $rm = 0$ for some non-zero $m \in M$.

(iii) The set of zero-divisors of M is denoted by $\mathcal{Z}(M)$, in other words,

$$\mathcal{Z}(M) = \bigcup_{\substack{m \in M \\ m \ne 0}} \mathrm{Ann}_R(m).$$

(iv) A prime ideal P of R is called an **associated prime ideal of** M if $P = \mathrm{Ann}_R(m)$ for some non-zero $m \in M$.

8.3 Lemma. Let M be a Noetherian R-module and N an R-submodule generated by the set S. Then N is generated by a finite subset of S.

Proof. Consider the (clearly non-empty) set of submodules of N generated by finite subsets of S. This set of submodules has a maximal element N', generated by $s_{i_1}, \dots, s_{i_n} \in S$. For any $s \in S$, the submodule of N generated by s, $s_{i_1}, \dots, s_{i_n}$ contains N' and is therefore equal to N' by maximailty of N'. We see that every $s \in S$ is already in N' and therefore $N = N'$. □

8.4 Remark: For any commutative ring R and R-module M, the set $R \setminus \mathcal{Z}(M)$ of non-zerodivisors of M is a saturated multiplicative set. Therfore, by 10.3, its complement, $\mathcal{Z}(M)$, is a union of prime ideals. In the Noetherian case, we will see that only finitely many prime ideals are needed.

8.5 Proposition (Prime and maximal annihilators). Let R be a commutative ring and $M \neq 0$ an R-module.

(i) Every maximal annihilator of a non-zero element is prime.

(ii) If R is Noetherian then every annihilator of a non-zero element is contained in a maximal one.

(iii) If M is a Noetherian module then there are only finitely many maximal annihilators of non-zero elements of M.

(iv) If R is a Noetherian ring and M a Noetherian module, then $\mathcal{Z}(M)$ is a finite union of prime ideals, each of which is an annihilator of a non-zero element of M:

$$\mathcal{Z}(M) = \mathrm{Ann}_R(m_1) \cup \ldots \cup \mathrm{Ann}_R(m_n), \quad \mathrm{Ann}_R(m_i) \text{ prime, for } 1 \leq i \leq n$$

Proof.
(i) Let $I = \mathrm{Ann}_R(m)$ be maximal among annihilators of non-zero elements. $I \neq R$ since M is unitary and non-zero. Suppose $ab \in I$ and $b \notin I$. Then $bm \neq 0$ and $a \in \mathrm{Ann}_R(bm)$. Now $\mathrm{Ann}_R(m) \subseteq \mathrm{Ann}_R(bm)$ implies, by maximality of I, that $\mathrm{Ann}_R(m) = \mathrm{Ann}_R(bm)$ and therefore $a \in I$.
(ii) For $I = \mathrm{Ann}_R(m)$, consider the set $\mathcal{S}$ of annihilators of non-zero elements containing I (which is non-empty since $I \in \mathcal{S}$). Since R is Noetherian $\mathcal{S}$ has a maximal element which is clearly maximal among annihilators of non-zero elements and contains I.
(iii) Suppose $P_\lambda = \mathrm{Ann}_R(m_\lambda)$, $\lambda \in \Lambda$ are all the maximal annihilators of non-zero elements of M. Consider the submodule N of M generated by the m_λ, $\lambda \in \Lambda$. There exists a finite subset $m_{\lambda_1}, \ldots, m_{\lambda_n}$ of these generators that already generate N. For any m_μ with $\mu \in \Lambda$ there exist $r_1, \ldots, r_n \in R$, such that $m_\mu = r_1 m_{\lambda_1}, + \ldots + r_n m_{\lambda_n}$, which implies $P_{\lambda_1} \ldots P_{\lambda_n} \subseteq Ann_R(m_\mu)$. Since $Ann_R(m_\mu) = P_\mu$ is prime we have $P_{\lambda_i} \subseteq P_\mu$ for some $1 \leq i \leq n$. By maximality of P_{λ_i} it follows that $P_\mu = P_{\lambda_i}$. Therfore every $\mathrm{Ann}_R(m_\mu)$, $\mu \in \Lambda$ is one of $P_{\lambda_1}, \ldots, P_{\lambda_n}$.
(iv) follows from (i)–(iii). □

8.6 Theorem. Let R be a Noetherian ring and M a Noetherian R-module. If I

is a subring (possibly without a unit) of R contained in $\mathcal{Z}(M)$ then there exists a non-zero element $m \in M$ with $Im = \{0\}$.

Proof. By the previous lemma, $\mathcal{Z}(M)$ is a union of finitely many prime ideals of the form $\mathrm{Ann}_R(m)$. By prime avoidance 8.1, I is contained in a single $\mathrm{Ann}_R(m)$. $\square$

8.7 Corollary (Universal zero divisor). Let R be a Noetherian ring, and I an ideal (or non-unitary subring) consisting entirely of zero-divisiors of R. Then there exists $r \in R$ such that $ir = 0$ for all $i \in I$.

$* * *$ *Associated primes* $* * *$

8.8 Definition. If M is an R-module, an **associated prime** of M is a prime ideal P of R that is the annihilator of an element of M, $P = \mathrm{Ann}(m)$. The set of all associated primes of M is denoted by $\mathrm{Ass}_R(M)$, or $\mathrm{Ass}(M)$, when R is understood.

8.9 Definition. The associated primes of an ideal I of an integral domain R are the associated primes of the R-module R/I.

The apparent ambiguity of the definition of the associated primes of an ideal I is not a problem, as the only associated prime of the R-module I is (0) (in an intergal domain, $\mathrm{Ann}(r) = 0$ for every non-zero $r \in R$), so this is a concept we can disregard.

Let R be an integral domain with quotient field K and $k \in K$. Consider the "conductor ideal" $(R{:}_R\, k) = \{r \in R \mid rk \in R\}$. Note that $(R{:}_R\, k) = R$ iff $k \in R$. Also, if k is written as a fraction of elements of R, $k = \frac{a}{b}$ then $(R{:}_R\, k) = (Rb{:}_R\, a)$, which is the annihilator of (the residue class of) a in R/Rb. Therefore conductor ideals (of elements of the quotient field) that are prime are exactly the associated primes of non-zero principal ideals of R.

9. *Motivation from algebraic geometry*

Let K be a field and $n \in \mathbb{N}$. We are interested in subsets of the n-dimensional K-vectorspace that are characterized by a system of polynomial equations in n variables with coefficients on K.

To every subset S of the polynomial ring $K[x_1, \ldots, x_n]$ we associate the set of its zeros

$$Z(S) = \{(a_1, \ldots, a_n) \in K^n \mid \forall f \in S\ f(a_1, \ldots, a_n) = 0\}$$

and to every subset A of the n-dimensional K-space the set of polynomials that are zero on A

$$I(A) = \{f \in K[x_1, \ldots, x_n] \mid \forall (a_1, \ldots, a_n) \in A\ f(a_1, \ldots, a_n) = 0\}.$$

We can consider Z as a function whose arguments are subsets of $K[x_1, \ldots, x_n]$ and whose values are subsets of K^n (and vice versa for I), or, without losing any information, we can restrict the arguments of Z and the values of I to ideals of $K[x_1, \ldots, x_n]$. This is so because $I(A)$ is an ideal of $K[x_1, \ldots, x_n]$ for every $A \subseteq K^n$, and $Z(S) = Z((S))$, where (S) is the ideal of $K[x_1, \ldots, x_n]$ generated by S, for every set of polynomials $S \subseteq K[x_1, \ldots, x_n]$. (Exercise: check this.)

Subsets of K^n of the form $A = Z(J)$ for some ideal $J \trianglelefteq K[x_1, \ldots, x_n]$ are called **algebraic** sets.

9.1 Remark: The more obvious properties of I and Z: For all $A, B \subseteq K[x_1, \ldots, x_n]$, and all $C, D \subseteq K^n$

(i) $A \subseteq B \implies Z(A) \supseteq Z(B)$ and $C \subseteq D \implies I(C) \supseteq I(D)$

(ii) $A \subseteq I(Z(A))$ and $C \subseteq Z(I(C))$

(iii) $Z(A) = Z(I(Z(A)))$ and $I(C) = I(Z(I(C)))$

(iv) There is a bijective correspondence between ideals of $K[x_1, \ldots, x_n]$ of the form $J = I(S)$ (for some $S \subseteq K^n$) and subsets of K^n of the form $A = Z(L)$ (for some ideal L of $K[x_1, \ldots, x_n]$) given by the restrictions of I and Z to arguments of this form.

(i) and *(ii)* are easy to see. By *(i)* and *(ii)*, I and Z constitute a Galois correspondence between subsets of K^n and ideals of $K[x_1, \ldots, x_n]$ (each ordered by set-theoretic inclusion). *(iii)* and *(iv)* then follow from the Galois correspondence.

9.2 Definition. A **Galois Correspondence** between two partially ordered sets $(\mathcal{X}, \leq)$ and $(\mathcal{Y}, \leq)$ consists of functions $f: \mathcal{X} \to \mathcal{Y}$ and $g: \mathcal{Y} \to \mathcal{X}$ satisfying the following conditions for all $A, B \in \mathcal{X}$ and all $C, D \in \mathcal{Y}$:

(i) $A \leq B \implies f(A) \geq f(B)$ and $C \leq D \implies g(C) \geq g(D)$

(ii) $A \leq f(g(A))$ and $C \leq g(f(C))$

9.3 Remark: The conditions defining a Galois correspondence are symmetric in f and g. To reflect this symmetry and to allow us to express two statements in one, we can write both f and g in prime notation: for $A \in \mathcal{X}$, $A' := f(A)$ and for $A \in \mathcal{Y}$, $A' := g(A)$. Conditions (i) and (ii) become

(i) $A \leq B \implies A' \geq B'$

(ii) $A \leq A''$

Given a Galois correspondence, we call an element A of $\mathcal{X}$ or $\mathcal{Y}$ **closed** with respect to the Galois correspondence, if it satisfies $A'' = A$.

It is easy to see that conditions (i) and (ii) above imply

(iii) $A' = A'''$,

which in turn implies

(iv) The subset of elements A in $\mathcal{X}$ (or $\mathcal{Y}$) satisfying $A = A''$ is exactly the subset of elements of the form B' for some $B \in \mathcal{Y}$ (or $\mathcal{X}$, respectively).

(v) There is a bijective correspondence, given by $A \mapsto A'$ (in either direction) between the set of closed elements in $\mathcal{X}$ and the set of closed elements in $\mathcal{Y}$.

*** *** ***

Like in other situations in mathematics, the nontrivial facts connected with a Galois correspondence between two sets consist of characterizations of the closed elements in either set from a different point of view, independent of the Galois structure.

The following Lemma shows that there is a topology on K^n whose closed sets are exactly the subsets of K^n of the form $Z(J)$ (for some ideal J of $K[x_1, \ldots, x_n]$).

9.4 Lemma.

1) If $A, B \subseteq K^n$ are algebraic sets then so is $A \cup B$. Indeed, for all sets $S, T \subseteq K[x_1, \ldots, x_n]$,

$$Z(S) \cup Z(T) = Z(ST),$$

where $ST = \{st \mid s \in S, t \in T\}$.

2) If A_λ is an algebraic set for all $\lambda \in \Lambda$ (an arbitrary index set) then $\bigcap_{\lambda\in\Lambda} A_\lambda$ is an algebraic set. Indeed,

$$\bigcap_{\lambda\in\Lambda} Z(S_\lambda) = Z(\bigcup_{\lambda\in\Lambda} S_\lambda).$$

3) $\emptyset$ and K^n are algebraic sets: $\emptyset = Z(1) = Z(K[x_1,\ldots,x_n])$ and $K^n = Z(0)$.

Proof. Ad 1) Clearly, $Z(S)\cup Z(T) \subseteq Z(ST)$. For the reverse inclusion, we consider a point $a \in Z(ST)$ that is not in $Z(S)$ and show that it is in $Z(T)$. Fix $s_0 \in S$ with $s_0(a) \neq 0$. For all $t \in T$, $0 = (s_0 \cdot t)(a) = s_0(a)t(a)$, therefore for all $t \in T$ $t(a) = 0$, i.e., $a \in Z(T)$.

Ad 2) $\bigcap_{\lambda\in\Lambda} Z(S_\lambda) = \{a \in K^n \mid \forall\lambda \in \Lambda\ \forall f \in S_\lambda f(a) = 0\} = Z(\bigcup_{\lambda\in\Lambda} S_\lambda)$. □

9.5 Remark:

1) If I and J are ideals of a ring R then IJ is defined as

$$IJ = \{i_1 j_1 + \ldots + i_k j_m \mid m \in \mathbb{N}, i_k \in I, j_k \in J\},$$

which is the ideal generated by $\{ij \mid i \in I, j \in J\}$.

With this definition of IJ, we have, for ideals I, J of $K[x_1,\ldots,x_n]$:

$$Z(I \cap J) = Z(IJ) = Z(I) \cup Z(J).$$

Proof: $\{ij \mid i \in I, j \in J\} \subseteq IJ \subseteq I \cap J$ implies $Z(I\cap J) \subseteq Z(IJ) \subseteq Z(\{ij \mid i \in I, j \in J\})$; $Z(\{ij \mid i \in I, j \in J\}) = Z(I) \cup Z(J)$ holds by lemma 9.4, and $Z(I)\cup Z(J) \subseteq Z(I\cap J)$ for purely logical reasons.

2) If S_λ is a subset of K^n for all $\lambda \in \Lambda$ then

$$I(\bigcup_{\lambda\in\Lambda} S_\lambda) = \bigcap_{\lambda\in\Lambda} I(S_\lambda).$$

In particular, for any set $A \subseteq K^n$,

$$I(A) = \bigcap_{a\in A} I(a).$$

9.6 Definition. Let R be a commutative ring and I an ideal of R. The **radical of** I is defined by

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

Note that $I \subseteq \sqrt{I}$ for every ideal I and that $\sqrt{I} = R$ if and only if $I = R$. It is easy to see that $\sqrt{Q} = Q$ whenever Q is a prime ideal or, more generally, an intersection of prime ideals. (We shall see in chapter 4 that $\sqrt{I}$ is the intersection of all prime ideals containing I.)

9.7 Theorem (Hilbert's Nullstellensatz). Let K be an algebraically closed field and $f_1, \ldots, f_m, g \in K[x_1, \ldots, x_n]$ such that $g(a) = 0$ for all $a \in Z(f_1, \ldots, f_m)$ then $g \in \sqrt{(f_1, \ldots, f_m)}$.

Proof. Will be proved in chapter 3. □

The importance of Hilbert's Nullstellensatz lies in the following corollary.

9.8 Corollary. Let J be an ideal of $K[x_1, \ldots, x_n]$, where K is an algebraically closed field. Then

$$I(Z(J)) = \sqrt{J}.$$

Proof. The Nullstellensatz says $I(Z(J)) \subseteq \sqrt{J}$ for finitely generated J, and from Hilbert's basis theorem we know that every ideal of $K[x_1, \ldots, x_n]$ is finitely generated. The reverse inclusion is easy; it holds even if K is not algebraically closed: if $g \in \sqrt{J}$ then for some $m \in \mathbb{N}$ $g^m \in J$ and therefore $g^m(a) = g(a) \ldots g(a) = 0$ for every $a \in Z(J)$. Since K is an integral domain, $g(a) = 0$ follows. □

9.9 Lemma (maximal ideals). Let K be a field, $a = (a_1, \ldots, a_n) \in K^n$, and define $M_{\bar{a}}$ to be the ideal of $K[x_1, \ldots, x_n]$ generated by $x_1 - a_1, \ldots, x_n - a_n$. Then $M_{\bar{a}} = I(\{a\})$ and $M_{\bar{a}}$ is a maximal ideal of $K[x_1, \ldots, x_n]$.

Proof. The substitution homomorphism $\varphi\colon K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ with $\varphi(x_i) = x_i - a_i$ and $\varphi(k) = k$ for $k \in K$ is an automorphism of $K[x_1, \ldots, x_n]$. Therefore the residue class ring of $M_{\bar{a}}$ is isomorphic to the residue class ring of $(x_1, \ldots, x_n)$, which is K. As K is a field, $M_{\bar{a}}$ is a maximal ideal. Therefore $M_{\bar{a}} \subseteq I(\{a\}) \subset K[x_1, \ldots, x_n]$ implies $M_{\bar{a}} = I(\{a\})$. □

With this in mind, $\sqrt{J} = I(Z(J))$ becomes

$$\sqrt{J} = \bigcap_{a \in Z(J)} I(a) = \bigcap_{J \subseteq I(a)} I(a) = \bigcap_{J \subseteq M_{\bar{a}}} M_{\bar{a}},$$

the statement that the radical of every ideal of $K[x_1, \ldots, x_n]$ (K algebraically closed) is an intersection of ideals of the form $M_{\bar{a}}$. (Since this also holds for maximal ideals, every maximal ideal is of the form $M_{\bar{a}}$.) Therefore, one way to see the Nullstellensatz is:

9.10 Theorem (Variant of Hilbert's Nullstellensatz). Let K be an algebraically closed field.

1. ("$K[x_1, \ldots, x_n]$ is a Hilbert ring.") In $K[x_1, \ldots, x_n]$, the radical of every ideal is an intersection of maximal ideals.
2. ("Weak Nullstellensatz") Every maximal ideal of $K[x_1, \ldots, x_n]$ is of the form $M_{\bar{a}}$, $a \in K^n$.

* * * * * * * * *

9.11 Definition. A subset Y of a topological space X is called **irreducible** if $Y \neq \emptyset$ and, whenever $Y \subseteq B \cup C$, where B, C are closed sets, it follows that $A \subseteq B$ or $A \subseteq C$.

For a closed set A, this is equivalent to: $A \neq \emptyset$; and, whenever $A = B \cup C$ with B, C closed, it follows that $A = B$ or $A = C$.

9.12 Remark: For a subset S of K^n with Zariski topology, S is **irreducible** if $S \neq \emptyset$ and, whenever $S \subseteq Z(J) \cup Z(L)$ for some $J, L \trianglelefteq K[x_1, \dots, x_n]$, it follows that $S \subseteq Z(J)$ or $S \subseteq Z(L)$.

For an algebraic subset $A = Z(I)$ of K^n this means: $A \neq \emptyset$ and, whenever $A = Z(J) \cup Z(L)$, it follows that $A = Z(J)$ or $A = Z(L)$.

9.13 Proposition. Let $A \subseteq K^n$. Then A is irreducible iff $I(A)$ is a prime ideal.

Proof. ($\Rightarrow$) Suppose A is irreducible and $JL \subseteq I(A)$ for some $J, L \trianglelefteq K[x_1, \dots, x_n]$; to show $J \subseteq I(A)$ or $L \subseteq I(A)$.

$$Z(J) \cup Z(L) = Z(JL) \supseteq Z(I(A)) \supseteq A$$

By irreducibility of A we get $A \subseteq Z(J)$ or $A \subseteq Z(L)$, say the former, which implies $I(A) \supseteq I(Z(J)) \supseteq J$.

($\Leftarrow$) Suppose $I(A)$ is prime and $A \subseteq Z(J) \cup Z(L)$; to show $A \subseteq Z(J)$ or $A \subseteq Z(L)$.

$$I(A) \supseteq I(Z(J) \cup Z(L)) = I(Z(J)) \cap I(Z(L)) \supseteq I(Z(J))I(Z(L))$$

$I(A)$ being prime we have $I(Z(J)) \subseteq I(A)$ or $I(Z(L)) \subseteq I(A)$, say the former. Then $A \subseteq Z(I(A)) \subseteq Z(I(Z(J))) = Z(J)$. $\square$

9.14 Corollary. For $I \trianglelefteq K[x_1, \dots, x_n]$, $Z(I)$ is irreducible iff $\sqrt{I}$ is prime.

The weak Nullstellensatz establishes a bijection between the points of K^n and the maximal ideals of $K[x_1, \dots, x_n]$ (when K is algebraically closed). Thus the topology on K^n (whose closed sets are the algebraic sets) translates to a topology on $\operatorname{MaxSpec}(K[x_1, \dots, x_n])$ (the set of maximal ideals of $K[x_1, \dots, x_n]$). A set S of maximal ideals is closed if and only if there exists an ideal I of $K[x_1, \dots, x_n]$ such that S is exactly the set of maximal ideals containing I.

This topology can be generalized to the spectrum of an arbitrary commutative ring R.

9.15 Definition. Let R be a commutative ring and $\operatorname{Spec}(R)$ the set of prime ideals of R. For every ideal I of R we define a set of prime ideals $V(I) = \{P \in \operatorname{Spec}(R) \mid I \subseteq P\}$.

Zariski topology on $\operatorname{Spec}(R)$ is defined by the convention: a set S of prime ideals of R is closed if and only if there exists an ideal I of R such that $S = V(I)$.

To show that this is a valid definition of a topology, we have to check:

9.16 Lemma.

1) Finite unions of closed sets are closed. Indeed, $V(I) \cup V(J) = V(IJ)$.
2) Arbitrary intersections of closed sets are closed. Indeed,

$$\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V((\bigcup_{\lambda \in \Lambda} I_\lambda)).$$

3) $\emptyset$ and $\operatorname{Spec}(R)$ are closed: $\emptyset = V(R)$ and $\operatorname{Spec}(R) = V((0))$.

We have a Galois connection between ideals of R on one hand and sets of prime ideals of R on the other hand given by $I \mapsto V(I)$ for $I \trianglelefteq R$ and $S \mapsto \bigcap_{P \in S} P$ for $S \subseteq \operatorname{Spec}(R)$, which gives a bijection between radical ideals of R and Zariski-closed sets of prime ideals.

It is clear that the Zariski-closure of a set S of prime ideals consists of all prime ideals containing $\bigcap_{P \in S} P$.

9.17 Definition. A topological space X is called Noetherian, if it satisfies the descending chain condition on closed sets, i.e., whenever $A_1 \supseteq A_2 \supseteq \dots A_m \supseteq A_{m+1} \supseteq \dots$ with A_i closed for all i, then there exists $N \in \mathbb{N}$ such that for all $i > N$ $A_i = A_N$.

9.18 Remark: It is easy to see that X is Noetherian if and only if every set $\mathcal{A}$ of closed sets has a minimal element with respect to inclusion.

If R is a Noetherian ring then $\operatorname{Spec}(R)$ with Zariski topology is easily seen to be a Noetherian topological space.

9.19 Theorem. Let X be a Noetherian topological space. Then every closed set A is a finite union of irreducible closed sets $A = A_1 \cup \dots \cup A_m$ with $A_i \subsetneq\!\!\!/ A_j$ for $i \neq j$ and these sets A_i are unique.

Proof. Existence: Suppose the set $\mathcal{A}$ of all closed sets that are not a finite union of closed irreducible sets is nonempty. Then it contains a mimimal A. This A is not irreducible, so there exist B, C closed with $A = B \cup C$ and $A \neq B$, $A \neq C$. By minimality of $A \in \mathcal{A}$, B and C are not in $\mathcal{A}$ and are each representable as a finite union of irreducible closed sets. But then, so is A, a contradiction. Once a closed set is represented as finite union of irreducible closed A_i we can delete those A_i that are contained in some A_j for $j \neq i$.

Uniqueness: Suppose $A_1 \cup \ldots \cup A_m = A'_1 cup \ldots \cup A'_n$. For $1 \leq i \leq m$ $A_i \subseteq A'_1 cup \ldots \cup A'_n$. As A_i is irreducible, there exists j with $A_i \subseteq A'_j$. By the same token, there exists k, such that $A'_j \subseteq A_k$. Then $A_i \subseteq A_k$. Therefore $i = k$ and $A_i = A'_j$. By setting $\varphi(i) = j$ with $A_i = A'_j$ we get an injective map $\varphi\colon \{1, \ldots m\} \to \{1, \ldots n\}$. φ is also surjective: take $k \in \{1, \ldots n\}$. Then, as above, there exists i with $A'_k = A_i$, and also $A_i = A'_{\varphi(i)}$, so $A'_k = A'_{\varphi(i)}$, which implies $k = \varphi(i)$. $\square$

10. *Primary ideals and the radical.*

*** *Multiplicatively closed setes.* ***

10.1 Definition. A non-empty subset S of a commutative ring R is called **multiplicatively closed**, or **multiplicative**, if $s,\, t \in S$ implies $st \in S$.

A multiplicatively closed set S is called **saturated** if it contains every divisor of each of its elements, i.e., if $s = ab \in S$ implies $a \in S$.

The set $\bar{S} = \{t \in R \mid \exists s \in S \;\; t \bigm| s\}$ of divisors of elements of a multiplicatve set S – clearly the smallest saturated multiplcative set containing S – is called the **saturation** of S.

Examples of multiplicatively closed sets (1–3 are saturated):
1) $R \setminus P$, where P is a prime ideal of R,
2) $R \setminus \bigcup_{\alpha \in A} P_\alpha$, where all P_α are prime ideals of R
3) the set of all non-zerodivisors in R
4) the set of powers of a fixed element $\{r^n \mid n \in \mathbb{N}_0\}$.

10.2 Lemma. Let S be a multiplicatively closed subset of R and I an ideal of R with $I \cap S = \emptyset$. Then there exists a prime ideal P of R with $I \subseteq P$ and $P \cap S = \emptyset$.

Proof. Apply Zorn's Lemma to $\mathcal{J} = \{J \trianglelefteq R \mid I \subseteq J \text{ and } S \cap J = \emptyset\}$. Since $I \in \mathcal{J}$, $\mathcal{J} \neq \emptyset$. Every chain of ideals in $\mathcal{J}$ has an upper bound in $\mathcal{J}$: its union is in $\mathcal{J}$. Let P be a maximal element of $\mathcal{J}$. We will show that P is prime. $S \neq \emptyset$ implies $P \neq R$. Suppose $ab \in P$, $a \notin P$ and $b \notin P$. By maximailty of P there exists $s \in S \cap (P + Ra)$ and $t \in S \cap (P + Rb)$. But then $st \in S \cap P$, a contradiction. □

10.3 Corollary.
(i) Let S be a saturated multiplicatively closed subset of R. Then $S = R \setminus \bigcup_{P \in \mathcal{P}} P$, where $\mathcal{P}$ is the set of all prime ideals P of R with $S \cap P = \emptyset$.
(ii) The saturated multiplicative subsets of R are precisely the complements of unions of prime ideals. (The trivial case $S = R$ corresponds to the empty union of prime ideals).

Proof. Ad (i). Clearly, $S \subseteq R \setminus \bigcup_{P \in \mathcal{P}} P$. For the reverse inclusion, we show that for every $u \notin S$ there exists some prime ideal P with $S \cap P = \emptyset$ and $u \in P$. S being saturated, $u \notin S$ implies $Ru \cap S = \emptyset$. By Lemma 10.2 there exists a prime ideal P with $Ru \subseteq P$ and $S \cap P = \emptyset$. Since the complement of a union of prime ideals is a saturated multiplicateve set, (ii) follows. □

10.4 Corollary. The set $\mathcal{Z}(R)$ of zero-divisors of a commutative ring R is a union of prime ideals of R. More generally, the set $\mathcal{Z}(M)$ of zero-divisors of any R-module M is a union of prime ideals of R.

Proof. Verify that $R \setminus \mathcal{Z}(R)$, and more generally, $R \setminus \mathcal{Z}(M)$, is a saturated multplicative set. $\square$

10.5 Lemma. Let I be an ideal of R and P a prime ideal containing I. Then there exists a minimal prime P' of I with $I \subseteq P' \subseteq P$.

Proof. Let $S = R \setminus P$ and consider the set $\mathcal{S}$ of multiplicatively closed sets T with $S \subseteq T$ and $T \cap I = \emptyset$. Then $\mathcal{S}$ is non-empty because $S \in \mathcal{S}$. Every chain of elements of $\mathcal{S}$ has an upper bound in $\mathcal{S}$ (its union). Let S_0 be a maximal element of $\mathcal{S}$ (which exists by Zorn's Lemma), and set $U = R \setminus S_0$. By Lemma 10.2, there exists a prime ideal P' containing I and disjoint from S_0, i.e., $I \subseteq P' \subseteq U$. It follows that $P' = U$ and P' is a minimal prime of I, since for any prime ideal Q with $I \subseteq Q \subsetneqq U$, its complement $R \setminus Q$ would be an element of $\mathcal{S}$ stricltly containing S_0. $\square$

$* * *$ *The radical.* $* * *$

10.6 Definition. Let I be an ideal of R. The **radical of** I is defined by

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

Convince yourself of the following easy facts:

10.7 Remark:
(1) $I \subseteq \sqrt{I}$
(2) $\sqrt{\sqrt{I}} = \sqrt{I}$
(3) $\sqrt{I} = R \iff I = R$
(4) If Q is an intersection of prime ideals then $\sqrt{Q} = Q$.

Recall that an element $r \in R$ is called **nilpotent** if there exists a natural number n with $r^n = 0$.

10.8 Definition. The radical of (0), consisting of all nilpotent elements of R, is called the **nilradical** of R:

$$\mathrm{Nil}(R) = \{r \in R \mid \exists n \in \mathbb{N} \ \ r^n = 0\}.$$

10.9 Proposition.

$$\sqrt{I} = \bigcap_{\substack{P \text{ prime} \\ I \subseteq P}} P.$$

Proof. Clearly, $\sqrt{I}$ is contained in all prime ideals containing I. Conversely, if $r \notin \sqrt{I}$, then $S = \{r^n \mid n \in \mathbb{N}\}$ is a multiplicatively closed set with $S \cap I = \emptyset$ and by Lemma 10.2, there exists a prime ideal P with $I \subseteq P$ and $r \notin P$. $\square$

10.10 Corollary. The nilradical of R is the intersection of all prime ideals of R.

10.11 Lemma. Some rules of arithmetic for radicals:

(1) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

(2) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$

(3) $\sqrt{I} + \sqrt{J} = R \iff I + J = R$

Proof. Exercise. $\square$

10.12 Lemma. Let P be a prime ideal of R and I an ideal of R.

(i) $P^n \subseteq I \subseteq P$ for some $n \in \mathbb{N}$ implies $\sqrt{I} = P$.

(ii) If R is Noetherian, then $\sqrt{I} = P$ implies for some n $P^n \subseteq I \subseteq P$.

Proof. (i) is easy. Ad (ii), $P = (p_1, \ldots, p_m) = \sqrt{I}$ implies for some $k \in \mathbb{N}$, $p_1^k, \ldots, p_m^k \in I$. Every element q of P is an R-linear combination of the p_i. By the multinomial theorem, $(r_1p_1 + \ldots + r_mp_m)^mk$ is a sum of terms each of which is divisible by p^k for some i, therefore $q^n \in I$ for every $q \in P$, $n = km$. $\square$

$* * *$ *Primary ideals* $* * *$

10.13 Definition. An ideal Q of R is called **primary** iff $Q \neq R$ and for all $a, b \in R$ with $ab \in Q$ either $a \in Q$ or $\exists n \in \mathbb{N}$ $b^n \in Q$.

The definition of primary tends to be confusing at first. If Q is primary, then $ab \in Q$ implies $a \in Q$ or $b \in \sqrt{Q}$, as well as, by symmetry, $b \in Q$ or $a \in \sqrt{Q}$. Therefore, for an ideal $Q \neq R$, being primary is equivalent to

$$ab \in Q \Rightarrow a \in Q \vee b \in Q \vee a, b \in \sqrt{Q}$$

10.14 Easy exercise. If Q is a primary ideal then $\sqrt{Q}$ is a prime ideal.

10.15 Definition. A primary ideal Q with $\sqrt{Q} = P$ is called **P-primary**.

Not every ideal whose radical is prime is primary, however. For instance, $\sqrt{P^n} = P$ for every prime ideal P and $n \in \mathbb{N}$, but not every power of a prime ideal is primary. In a more positive vein, we have the following facts:

10.16 Lemma. Let M be a maximal ideal of R and Q an ideal with $\sqrt{Q} = M$. Then Q is M-primary.

Proof. Suppose $ab \in Q$ and $a \notin M$; we must show $b \in Q$. We have $M + aR = R$, i.e., $\sqrt{Q} + aR = R$. This implies $Q + aR = R$, so $1 = q + ar$ for some $q \in Q$ and $r \in R$, and finally $b = qb + abr \in Q$. $\square$

10.17 Corollary. Let M be a maximal ideal of R and $I \neq R$ an ideal with $M^n \subseteq I$ for some $n \in \mathbb{N}$. Then I is M-primary.

Proof. I is not contained in any prime ideal P other than M: if $I \subseteq P$ then for every $m \in M$, $m^n \in I \subseteq P$ implies $m \in P$, hence $M = P$. Since $I \neq R$, this shows $\sqrt{I} = M$ and we are done. $\square$

Just like prime ideals, primary ideals behave nicely with respect to ring homomorphisms:

10.18 Lemma. Let $f\colon R \to T$ be a ring homomorphism (with $f(1) = 1$, as always) and I, Q ideals of T. Then

(1) $f^{-1}(\sqrt{I}) = \sqrt{f^{-1}(I)}$.

(2) If Q is P-primary then $f^{-1}(Q)$ is $f^{-1}(P)$-primary.

Again, like prime ideals, primary ideals can be characterized by a property of their quotient ring.

10.19 Proposition. An ideal Q is primary if and only if R/Q is a non-zero ring in which every zero-divisor is nilpotent.

Proof. Easy. $\square$

Together with the previous lemma this implies that a canonical projection induces a bijection between primary ideals containing the kernel and primary ideals in the quotient ring. (Note that everything we show for canonical projections holds mutatis mutandis for any surjective ring homomorphism $f\colon R \to T$, since f is just the canonical projection $\pi\colon R \to R/\mathrm{Ker} f$ followed by the isomorphism $\bar{f}\colon R/\mathrm{Ker} f \to T$.)

10.20 Proposition. Let I be an ideal of R and $\pi\colon R \to R/I$ the canonical projection. Then a bijection between all primary ideals Q of R with $I \subseteq Q$ and all primary ideals of R/I is given by $Q \mapsto \pi(Q)$. Its inverse is $\tilde{Q} \mapsto \pi^{-1}(\tilde{Q})$ (for $\tilde{Q} \trianglelefteq R/I$).

Primary ideals also behave just like prime ideals with respect to the canonical homomorphism into a ring of fractions $f_S\colon R \to R_S$ and with respect to the canonical projection onto a residue class ring:

10.21 Proposition. Let R_S be a ring of fractions of R and $f_S\colon R \to R_S$ the canonical homomorphism.

(1) If $Q \trianglelefteq R$ is primary and $\frac{r}{s} \in Q_S$ then $r \in Q$.

(2) A bijection between the primary ideals Q of R with $S \cap Q = \emptyset$ and all primary ideals of R_S is given by $Q \mapsto Q_S$ (for Q a primary ideal of R). Its inverse is $\tilde{Q} \mapsto f_S^{-1}\tilde{Q}$ (for $\tilde{Q}$ a primary ideal of R_S).

This is shown just like the analogous statement for prime ideals. (Note that $Q \cap S = \emptyset$ implies $\sqrt{Q} \cap S = \emptyset$.)

∗ ∗ ∗ Goldman-Krull proof of Hilbert's Nullstellensatz ∗ ∗ ∗

If P is an ideal of a commutative ring R, we know that

$$P \text{ is prime } \iff R/P \text{ is an integral domain}$$
$$P \text{ is maximal } \iff R/P \text{ is a field.}$$

We are now going to see a similar characterization for a concept that falls in between prime and maximal.

P is a prime ideal that is not an intersection of strictly larger prime ideals.	$\iff$	R/P is an integral domain whose quotient field is generated (as a ring over R/P) by a single element.

11.1 Definition. An ideal P is a **G-ideal** (or **Goldman-ideal**) if P is a prime ideal which is not an intersection of prime ideals strictly containing P.

Note that P is a G-ideal iff R/P is an integral domain in which the intersection of all non-zero prime ideals is not (0).

11.2 Definition. A domain D with quotient field K is a **G-domain** if K is generated by a single element as a ring over D, i.e., $\exists z \in K$ such that $K = D[z]$.

Some equivalent characterizations of G-domains:

11.3 Lemma. Let D be a domain and K its quotient field. The following are equivalent:

(1) There exists $u \in D \setminus \{0\}$ such that $K = D[u^{-1}]$.
(2) K is generated by a single element as a ring over D.
(3) K is finitely generated as a ring over D.

Proof. $(3 \Rightarrow 1)$ If $K = D[\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}]$ and $u = b_1 \cdot \ldots \cdot b_n$ then $K = D[u^{-1}]$. □

11.4 Lemma. Let D be a domain, K its quotient field, and $0 \neq u \in D$. Then $K = D[u^{-1}]$ iff u is in the intersection of all prime ideals $P \neq (0)$ of D.

Proof. Suppose $K = D[u^{-1}]$ and let P be a non-zero prime ideal. Pick $b \in P \setminus \{0\}$. Then $b^{-1} = cu^{-n}$ for some $c \in D$ and $n \in \mathbb{N}$. Now $bc = u^n$, therefore $u^n \in P$ and finally $u \in P$.

Conversely, suppose $u \in P$ for every prime ideal $P \neq (0)$. Let $0 \neq b \in D$. Then $u \in \sqrt{Rb}$, meaning there exists $n \in \mathbb{N}$ with $u^n = cb$ for some $c \in D$. Rewritten as $b^{-1} = cu^{-n}$ this shows $b^{-1} \in D[u^{-1}]$. As b was arbitrary, $K = D[u^{-1}]$. □

As a consequence of the previous two lemmata:

11.5 Theorem. Let D be a domain. The intersection of all non-zero prime ideals of D is not (0) iff the quotient field of D is generated by a single element as a ring over D.

Applying this to residue class rings we get:

11.6 Corollary. Let $P \trianglelefteq R$. Then P is a G-ideal iff R/P is a G-domain.

Note that a commutative ring R is a G-domain if and only if (0) is a G-ideal of R.

11.7 Lemma. Let I be an ideal in a commutative ring R. Then

$$\sqrt{I} = \bigcap_{\substack{P \text{ G-ideal} \\ I \subseteq P}} P.$$

Proof. Clearly, $\sqrt{I}$ is contained in every prime ideal containing I. Conversely, if $u \notin \sqrt{I}$ then there exists a G-ideal P containing I with $u \notin P$: As in the proof of $\sqrt{I} = \bigcap_{I \subseteq P \text{ prime}} P$ (10.9), let P be maximal among the ideals containing I and disjoint with $S = \{u^n \mid n \in \mathbb{N}\}$. Then P is prime. Also, P is a G-ideal, because every prime ideal strictly containing P intersects S and therefore contains u, but $u \notin P$. □

11.8 Lemma and Definition. Let R be a commutative ring. Then the following are equivalent

1) Every G-ideal of R is maximal.
2) For every ideal I of R, $\sqrt{I}$ is an intersection of maximal ideals.

A commutative ring satisfying one (and hence both) of the above conditions is called **Hilbert ring** (or **Jacobson ring**).

Proof. $(2 \Rightarrow 1)$ Let P be a G-ideal. Then $\sqrt{P} = P$, because P is prime. By 2), P is an intersection of maximal ideals, but, as a G-ideal, P is no intersection of prime ideals strictly containing P, therefore P must be maximal. □

11.9 Lemma. Let R be a commutative ring. Then $R[x]$ is not a G-domain.

Proof. If R is not a domain, then $R[x]$ is not a domain, let alone a G-domain. Now let R be a domain with quotient field K. We must show that the intersection of all non-zero prime ideals of $R[x]$ is (0).

Since $P \cap R[x]$ is a non-zero prime ideal of $R[x]$ for every non-zero prime ideal P of $K[x]$, it suffices to show that the intersection of all non-zero prime ideals of $K[x]$ is (0).

This is the case because there are infinitely many monic irreducible polynomials in $K[x]$: If there were only finitely many, $p_1 = x, p_2, \ldots, p_n$, then $p_1 \cdot \ldots \cdot p_n + 1$ (which is not a unit because its degree is not zero), would not be divisible by any monic irreducible polynomial, a contradiction to $K[x]$ being a unique factorization domain. □

11.10 Corollary. Let K be a field. Then $K[x]$ is a Hilbert ring.

Proof. $K[x]$ is a principal ideal domain, so the only non-maximal prime ideal is (0), which is not a G-ideal by 11.9. Therefore every G-ideal of $K[x]$ is maximal. □

11.11 Lemma. Let $S \subseteq T$ be domains, $T = S[t]$ with t algebraic over S. Then T is a G-domain if and only if S is a G-domain.

Proof. Let K and L be the quotient fields of S and T respectively. Then $L = K[t]$ is algebraic over K (and hence over S). Suppose T is a G-domain. Then $L = T[c^{-1}] = S[t, c^{-1}]$ for some $c \in T$. Both c^{-1} and t are algebraic over S. Let a and b be the leading coefficients of non-zero polynomials f and g in $S[x]$ with $f(c^{-1}) = 0$ and $g(t) = 0$ and let $\tilde{S} = S[a^{-1}, b^{-1}]$. Then c^{-1} and t are integral over $\tilde{S}$. Hence L is integral over $\tilde{S}$, which makes $\tilde{S}$ a field (4.17). Clearly, $\tilde{S} = K$. Therefore K is finitely generated as a ring over S, and S is a G-domain.

The converse is easy. If S is a G-domain then $K = S[s^{-1}]$ for some $s \in S$ and the quotient field of $T = S[t]$ (with t algebraic over S) is $K(t) = K[t] = S[s^{-1}, t] = T[s^{-1}]$. □

11.12 Lemma. Let R be a commutative ring. If Q is a G-ideal of $R[x]$ then $P = Q \cap R$ is a G-ideal of R.

Proof. Let Q be a G-ideal of $R[x]$ and $P = Q \cap R$. Then Q contains $P[x]$ and this containment is strict, because $R[x]/Q$ is a G-domain by hypothesis and $R[x]/P[x] \simeq (R/P)[x]$ is not a G-domain by Lemma 11.9.

Let $S = R/P$ and $T = R[x]/Q$. We know that T is a G-domain and want to show that S is a G-domain.

S is contained in T via $r + P \mapsto r + Q$, which is injective, because $P = Q \cap R$. Also, $T = S[t]$ for $t = x + Q$.

We show that t is algebraic over S: Clearly, $t = x + Q \in T$ is a root of f for any $f \in Q$, and there exists some $f \in Q$ which is not the zero polynomial in $(R/P)[x]$, because $Q \supsetneqq PR[x]$. We can now apply Lemma 11.11. $\square$

11.13 Lemma. Let R be a commutative ring and P a G-ideal of R. Then there exists a maximal ideal M of $R[x]$ with $M \cap R = P$.

Proof. Let $S = R/P$ and K the quotient field of S. As S is a G-domain, $K = S[b]$ for some $b \in K$. Let $\pi\colon S[x] \to S[b]$ be the substitution homomorphism with $\pi(x) = b$, $\pi\big|_S = \mathrm{id}_S$. Since the image of π, $S[b]$, is a field, the $\mathrm{Ker}(\pi) = M$ is a maximal ideal of $S[x]$, and clearly $\mathrm{Ker}(\pi) \cap S = (0)$.

Now $S[x] = (R/P)[x] \simeq R[x]/P[x]$, and every maximal ideal M of $R[x]/P[x]$ corresponds to a maximal ideal Q of $R[x]$ containing $P[x]$ (the inverse image of M under the canonical projection of $R[x]$ onto $(R/P)[x]$, and $M \cap S = (0)$ translates to $Q \cap R = P$. $\square$

Lemma 11.13 and Lemma 11.12 combined yield:

11.14 Theorem. Let R be a commutative ring and P an ideal of R. The following are equivalent:

(1) P is a G-ideal of R.

(2) There exists a maximal ideal M of $R[x]$ with $M \cap R = P$.

(3) There exists a G-ideal Q of $R[x]$ with $Q \cap R = P$.

11.15 Proposition. Let R be a commutative ring.

(1) $R[x]$ is a Hilbert ring if and only if R is a Hilbert ring.

(2) If R is a Hilbert ring, then every maximal ideal Q of $R[x]$ is generated by $P = Q \cap R$ together with some $f \in R[x]$, which represents an irreducible polynomial in $(R/P)[x]$.

Proof. Suppose R is a Hilbert ring, Q a G-ideal of $R[x]$, and $P = Q \cap R$.

$P = Q \cap R$ is a G-ideal of R by 11.12, and hence maximal by hypothesis. Q is the inverse image of some G-ideal $\bar{Q}$ of $R[x]/PR[x] \simeq (R/P)[x]$ under the canonical projection $\pi : R[x] \to R[x]/PR[x]$. As $(R/P)[x]$ is the polynomial ring over a field, $\bar{Q}$ is maximal by 11.10, and therefore Q is a maximal ideal of $R[x]$.

Furthermore, $\bar{Q}$ is generated by a single irreducible polynomial in $\bar{f} \in (R/P)[x]$, so Q is generated by P and f, a representative in $R[x]$ of $\bar{f}$.

We have shown (2), and the "if" direction of (1). The "only if" direction of (1) is easy: R is a homomorphic image of $R[x]$ and the Hilbert ring property clearly carries over to homomorphic images. $\square$

11.16 Theorem. Let K be an algebraically closed field and $n \in \mathbb{N}$. Then

(1) $K[x_1, \ldots, x_n]$ is a Hilbert ring.

(2) Every maximal ideal of $K[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$, for some $a_1, \ldots, a_n \in K$.

Proof. (1) follows from 11.15 by induction. (Note that a field is trivially a Hilbert ring: every prime ideal is maximal.)

Similarly, we show (2) by induction, using 11.15: $n = 1$: if K is algebraically closed, every maximal ideal of $K[x]$ is generated by a monic linear polynomial.

Now let M be a maximal ideal of $K[x_1, \ldots, x_n]$ and $P = M \cap K[x_1, \ldots, x_{n-1}]$. P is a G-ideal by 11.12, and hence maximal by (1). $P = (x_1 - a_1, \ldots, x_{n-1} - a_{n-1})$, by induction hypothesis, therefore $K[x_1, \ldots, x_{n-1}]/P \simeq K$, and every irreducible polynomial of $(K[x_1, \ldots, x_{n-1}]/P)[x_n]$ has the form $x_n - (a_n + P)$, for some $a_n \in K$.

Applying part (2) of 11.15 to $R = K[x_1, \ldots, x_{n-1}]$, M is generated by $x_1 - a_1, \ldots, x_{n-1} - a_{n-1}$ and $x_n - a_n$. □

11.17 Corollary (Version of Hilbert's Nullstellensatz). Let K be an algebraically closed field and $I \trianglelefteq K[x_1, \ldots, x_n]$. Then $\sqrt{I}$ is the intersection of all ideals of the form $M_a = \{f \in K[x_1, \ldots, x_n] \mid f(a) = 0\}$ (with $a \in K^n$) containing I.

11.18 Corollary (Hilbert's Nullstellensatz). Let K be an algebraically closed field and $n \in \mathbb{N}$. If $f_1, \ldots, f_m, g$ are polynomials in $K[x_1, \ldots, x_n]$ such that $g(a) = 0$ for all $a \in K^n$ for which $f_i(a) = 0$ for $1 \leq i \leq m$ then $g \in \sqrt{(f_1, \ldots, f_m)}$.

$* * *$ *classical proof of Hilbert's Nullstellensatz* $* * *$

11.19 Lemma. Let $K \subseteq F$ be fields. If $F = K[z_1, \ldots, z_n]$ (F is generated by $z_1, \ldots, z_n$ as a ring over K) then $z_1, \ldots, z_n$ are algebraic over K.

Proof. Induction on n. If x is transcendental over K then the polynomial ring $K[x]$ is not a field (every polynomial of positive degree is a non-unit).

Now let $F = K[z_1, \ldots, z_n]$, $n > 1$. $F = K(z_1)[z_2, \ldots, z_n]$, so by induction hypothesis $z_2, \ldots, z_n$ are algebraic over $K(z_1)$. There exists an element $r \in K[z_1]$ ($r = g(z_1)$ for some $g \in K[x]$) such that $rz_2, \ldots, rz_n$ are integral over $K[z_1]$. Therefore, for every $f \in K[z_1, \ldots, z_n]$ there exists $m \in \mathbb{N}$ such that $r^m f$ is integral over $K[z_1]$. In particular, this holds for every $f \in K(z_1) \subseteq K[z_1, \ldots, z_n]$.

Suppose z_1 is transcendental over K. Then $K[z_1]$ is a unique factorization domain with infinitely many irreducibles. $K[z_1]$ is integrally closed in its quotient field $K(z_1)$. By the previous paragraph, every element of $K(z_1)$ has a representation as a fraction whose denominator is a power of a fixed polynomial $g(z_1)$. This is false. Therefore, z_1 is algebraic over K. $\square$

11.20 Theorem (weak Nullstellensatz). Let K be an algebraically closed field. Then every maximal ideal of $K[x_1,\dots,x_n]$ is of the form $(x_1-a_1,\dots,x_n-a_n)$ for some $a_1,\dots,a_n\in K$.

Proof. Let M be a maximal ideal of $K[x_1,\dots,x_n]$, and $F=K[x_1,\dots,x_n]/M$ the residue field. The canonical projection $\pi\colon K[x_1,\dots,x_n]\longrightarrow K[x_1,\dots,x_n]/M$, restricted to K is injective, so the elements $k+M$ (with $k\in K$) form an isomorphic copy of K in F, and F is generated as a ring over K by the images of the x_i under π, $F=K[y_1,\dots,y_n]$, with $y_i=x_i+M$.

By 11.19, $y_1,\dots,y_n$ are algebraic over K. As K is algebraically closed, the only monic irreducible polynomials in $K[x]$ are linear, so each y_i is a zero of $x-a_i$ for some $a_i\in K$, i.e., $(x_i+M)-(a_i+M)=0+M$. This implies $x_i-a_i\in M$ for $1\le i\le n$. Since the ideal generated by x_1-a_1, …, x_n-a_n is maximal, it must be M. $\square$

A really neat argument by Rabinowitsch shows that the Nullstellensatz for n variables follows from the weak Nullstellensatz for $n+1$ variables:

11.21 Theorem. Let K be an algebraically closed field, and $f_1,\dots,f_m,f$ polynomials in $K[x_1,\dots,x_n]$ such that $f(a)=0$ for every common zero $a\in K^n$ of $f_1,\dots,f_m$. Then $f\in\sqrt{(f_1,\dots,f_m)}$.

Proof. Let $f_1,\dots,f_m,f\in K[x_1,\dots,x_n]$ as in the theorem. The polynomials $f_1,\dots,f_m$ and $g=1-x_{n+1}f$ in $K[x_1,\dots,x_{n+1}]$ have no common zero in K^{n+1}. By the weak Nullstellensatz they are not contained in any maximal ideal of $K[x_1,\dots,x_{n+1}]$, so there exist $h_1,\dots,h_m,h\in K[x_1,\dots,x_{n+1}]$ such that

$$f_1h_1+\ldots+f_mh_m+(1-x_{n+1}f)h=1.$$

We now substitute $1/f$ for x_{n+1} and multiply both sides by f^r, where r is the maximal degree in x_{n+1} of any h_i. This gives $f_1g_1+\ldots+f_mg_m=f^r$, where $g_1,\dots,g_m\in R[x_1,\dots,x_n]$, so f is in the radical of the ideal generated by $f_1,\dots,f_m$ in $K[x_1,\dots,x_n]$. $\square$

12. *A little point-set topology.*

*** *Open and closed sets* ***

12.1 Definition. A subset τ of the power set $\mathcal{P}(X)$ of a set X is called a **topology** on X if the following axioms hold:

(O1) $\emptyset \in \tau$ and $X \in \tau$

(O2) $S, T \in \tau \implies S \cap T \in \tau$

(O3) $S_i \in \tau$ for all $i \in I$ (I an arbitrary index set) $\implies \bigcup_{i \in I} S_i \in \tau$

(X, τ) is then called a **topological space**. The members of τ are called **open sets**.

If (X, τ) is a topological space, then the complements of open sets, $A = X \setminus S$ with $S \in \tau$, are called **closed sets**. The collection of closed sets $\mathcal{C} = \{X \setminus O \mid O \in \tau\}$ satisfies

(C1) $\emptyset \in \mathcal{C}$ and $X \in \mathcal{C}$.

(C2) $A, B \in \mathcal{C} \implies A \cup B \in \mathcal{C}$.

(C3) $A_i \in \mathcal{C}$ for all $i \in I$ (I an arbitrary index set) $\implies \bigcap_{i \in I} A_i \in \mathcal{C}$

Conversely, if $\mathcal{C} \subseteq \mathcal{P}(X)$ satisfys C1–C3, then the complements of elements of $\mathcal{C}$ form a topology on X, whose closed sets are precisely the elements of $\mathcal{C}$.

12.2 Example: Zariski topology on the spectrum of a ring. Let R be a commutative ring. A topology on the spectrum of R ($\mathrm{Spec}(R) = \{P \mid P$ a prime ideal of $R\}$) is defined by specifying its closed sets as sets of prime ideals of the form

$$V(I) = \{P \in \mathrm{Spec}(R) \mid P \supseteq I\},$$

for some ideal I of R.

There's nothing to prevent sets from being open and closed at the same time. Sets both open and closed are often called **clopen**.

12.3 Definition. Let (X, τ) be a topological space.

A collection $\mathcal{B}$ of open sets such that every open set is a union of elements of $\mathcal{B}$ is called a **basis** of the topology τ.

A collection $\mathcal{S}$ of open sets such that every open set is a union of finite intersections of elements of $\mathcal{S}$ is called a **subbasis** of the topology τ.

Topologies can be defined by specifying a basis or subbasis: If $\mathcal{B} \subseteq \mathcal{P}(X)$ is closed with respect to finite intersections, then the unions of (arbitrarily many) members of $\mathcal{B}$ form a topology on X, of which $\mathcal{B}$ is a basis.

If $\mathcal{S} \subseteq \mathcal{P}(X)$ is any collection of subsets of X, then arbitrary unions of finite intersections of members of $\mathcal{S}$ form a topology on X, of which $\mathcal{S}$ is a subbasis.

12.4 Example: Order Topology. If $(X, \leq)$ is a totally ordered set, then **order topology** on X is defined by specifying "open rays", i.e., sets of the form $(a, \infty) = \{x \in X \mid a < x\}$ and $(-\infty, b) = \{x \in X \mid x < b\}$, for $a, b \in X$ as a subbasis.

If $(X, \leq)$ has neither a maximal nor a minimal element, then "open intervals" $(a, b) = \{x \in X \mid a < x < b\}$ form a basis of order topology. (If X does have a maximal or minimal element, then open rays of the form (a, ∞), or $(-\infty, b)$, respectively, have to be added to the open intervals to get a basis.)

12.5 Definition. If (X, τ) is a topological space and Y a subset of X then Y inherits a topological structure from X (called **subspace topology**) through the convention: a subset U of Y is open (in Y) iff there exists an open subset O of X with $U = O \cap Y$.

If Y is an open subset of X then $U \subseteq Y$ is open in Y if and only it is open in X; if Y is a closed subset of X then $A \subseteq Y$ is closed in Y if and only it is closed in X.

12.6 Remark: If $(X, \leq)$ is a totally ordered set and $Y \subseteq X$, then Y inherits a topology from the order topology of X, and at the same time Y inherits an order relation from X which makes $(Y, \leq)$ a totally ordered set, for which order topology may be defined. These two topologies on Y in general do not agree. (Examples can be found among subsets of the real numbers.)

$***$ *Neighborhoods and neighborhood bases* $***$

Perhaps a more intuitive approach to topology is through neighborhoods of a point, which (as sets containing an open ball around the point) are already familiar from the study of metric spaces.

12.7 Definition. $(*)$ Let (X, τ) be a topological space and $p \in X$. A neighborhood of p is a set U such that there exists an open set O with $p \in O \subseteq U$. The set of all neighborhoods of a point p is called the **neighborhood filter** of p. We will denote it by $\mathcal{U}(p)$.

12.8 Remark: Let (X, τ) be a topological space and $p \in X$. The neighborhood filter of p has the properties

(U1) $\forall U \in \mathcal{U}(p) \ \ p \in U$.

(U2) $U, V \in \mathcal{U}(p) \implies U \cap V \in \mathcal{U}(p)$

(U3) $U \in \mathcal{U}(p)$ and $V \supseteq U \implies V \in \mathcal{U}(p)$

(U4) $\forall U \in \mathcal{U}(p)\ \exists V \in \mathcal{U}(p)\ \forall v \in V\ \ U \in \mathcal{U}(v)$.

Also,

$$(U) \qquad O \in \tau \iff \forall p \in O\ \ \exists U \in \mathcal{U}(p)\ \ U \subseteq O$$

Conversely, given a set X and for each $p \in X$ a set $\mathcal{U}(p) \subseteq \mathcal{P}(X)$ such that U1–U4 hold, we can define a topolgy τ on X by (U), and, what is more, the neighborhood filter of each point in the resulting topology τ is exactly the $\mathcal{U}(p)$ we started out with.

As with metric spaces, it suffices to know a system of "basic" neighborhoods of a point – with the property that every neighborhood contains one of them – to know all neighborhoods.

12.9 Definition. Let (X, τ) be a topological space. A collection $\mathcal{B}(p) \subseteq \mathcal{U}(p)$ of neighborhoods of p is called a **neighborhood basis** of p if for every $U \in \mathcal{U}(p)$ there exists $B \in \mathcal{B}(p)$ with $B \subseteq U$.

If (X, τ) is a topological space, and for each $p \in X$, $\mathcal{B}(p)$ is a neighborhood basis, then, for every $p \in X$

(B1) $\forall B \in \mathcal{B}(p)\ \ p \in B$.

(B2) $U, V \in \mathcal{B}(p) \implies \exists B \in \mathcal{B}(p)\ \ B \subseteq U \cap V$

(B3) $\forall U \in \mathcal{B}(p)\ \exists V \in \mathcal{B}(p)\ \forall v \in V\ \exists B \in \mathcal{B}(v)\ B \subseteq U)$.

Also,

$$(B) \qquad O \in \tau \iff \forall p \in O\ \ \exists B \in \mathcal{B}(p)\ \ B \subseteq O$$

Conversely, if we are given for every $p \in X$ a collection $\mathcal{B}(p)$ of subsets of X satisfying B1–B3, we can define a topology on X by (B), and in this topology $\mathcal{B}(p)$ will be a neighborhood basis of p.

12.10 Definition. A topological space in which every point has a countable neighborhood basis is said to satisfy the **first countability axiom**.

12.11 Example: Let (X, d) be a metric space, and $B_\varepsilon(p) = \{x \in X \mid d(p, x) < \varepsilon\}$ (for $\varepsilon > 0$, $p \in X$) the open ball of radius ε around p. If we define $\mathcal{B}(p)$ as the set of all $B_\varepsilon(p)$ with $\varepsilon > 0$, then B1–B3 hold. In other words, every metric induces a topology in which the open ε-balls with center p form a neighborhood basis of p. Actually, countably many balls $B_{\frac{1}{n}}(p)$, $n \in \mathbb{N}$, already form a neighborhood basis of p in this topology. We see that every metric space satisfies the first countability axiom.

12.12 Example: I-adic topology Let R be a commutative ring and I an ideal of R. I-adic topology on R is defined by specifying a neighborhood base of $r \in R$:

$$\mathcal{B}(r) = \{r + I^n \mid n \in \mathbb{N}\}.$$

Note that these basic neighborhoods are both open and closed.

$* * *$ *Closure and interior* $* * *$

12.13 Definition. Let A be a subset of a topological space X. The **closure** of A, denoted $\bar{A}$, is defined to be the intersection of all closed sets containing A.

Clearly, $\bar{A}$ is a closed set containing A and every closed set B that contains A also contains $\bar{A}$.

The **closure operator** $A \mapsto \bar{A}$ on $\mathcal{P}(X)$ has the properties:

(A1) $\bar{\emptyset} = \emptyset$.

(A2) $A \subseteq \bar{A}$.

(A3) $\bar{\bar{A}} = \bar{A}$.

(A4) $\bar{A} \cup \bar{B} = \overline{A \cup B}$.

Conversely, any operator $A \mapsto \bar{A}$ on the power set of a set X with properties A1–A4 may be used to define a topology on X by declaring the closed sets to be precisely the sets of the form $\bar{A}$ for some $A \in \mathcal{P}(X)$. (To see that these sets satisfy C3, first note that A4 implies $A \subseteq C \implies \bar{A} \subseteq \bar{C}$. From this we get that $\overline{\bigcap_{i \in I} \bar{A}_i} \subseteq \bar{A}_i$ for all $i \in I$, i.e., $\overline{\bigcap_{i \in I} \bar{A}_i} \subseteq \bigcap_{i \in I} \bar{A}_i$ and the reverse inclusion is just A2.)

12.14 Definition. Let (X, τ) be a topological space and $A \in \mathcal{P}(X)$ then the **open interior** (or **interior** for short) of A, denoted A°, is the union of all open sets contained in A.

Clearly, A° is open and $A^\circ \subseteq A$. Also, $(X \setminus A)^\circ = X \setminus \bar{A}$. (Note that the interior of a non-empty set may be empty.)

$* * *$ *Boundry points, accumulation points and such* $* * *$

The following properties of the closure of a set (which we defined as the intersection of all closed sets containing it) and the interior of a set (which we defined as the union of all open sets contained in it) are often used as definitions:

12.15 Lemma.

- $\bar{A}$ consists of precisely those points $p \in X$ such that $U \cap A \neq \emptyset$ for every neighborhood $U \in \mathcal{U}(p)$ and
- A° consists of precisely those points $p \in X$ such that there exists a neighborhood $U \in \mathcal{U}(p)$ with $U \subseteq A$.

12.16 Definition. Let (X, τ) be a topological space, $p \in X$ and $A \subseteq X$ then

- p is called a **boundary point** of A if for every neighborhood $U \in \mathcal{U}(p)$ both $A \cap U \neq \emptyset$ and $(X \setminus A) \cap U \neq \emptyset$. The set of all boundary points of A is the **boundary** of A, denoted by δA.
- p is called an **interior point** of A if $p \in A^\circ$, i.e., if there exists a neighborhood $U \in \mathcal{U}(p)$ with $U \subseteq A$.
- p is called an **accumulation point** of A if every neighborhood of p contains an element of A other than p.
- p is called an **isolated point** of A if there exists a neighborhood U of p with $U \cap A = \{p\}$.

Note that interior points of A and isolated points of A are necessarily in A, while boundary points and accumulation points may or may not belong to A.

By purely logical arguments we see that every set A induces a partition of X into three disjoint parts in two different ways ($\dot\cup$ denotes disjoint union):

(i) $X = A^\circ \,\dot\cup\, \delta A \,\dot\cup\, (X \setminus A)^\circ$ and

(ii) $X = \{\text{isolated points of } A\} \dot\cup \{\text{accumulation points of } A\} \dot\cup (X \setminus A)^\circ$.

Also,

(iii) $\bar{A} = A^\circ \,\dot\cup\, \delta A$ and

(iv) $\bar{A} = \{\text{isolated points of } A\} \,\dot\cup\, \{\text{accumulation points of } A\}$

The last two partitions of $\bar{A}$ follow from the characterization of $\bar{A}$ as the set of those p such that $A \cap U \neq \emptyset$ for every $U \in \mathcal{U}(p)$. They are incomparable in the sense that all four combinations of belonging to one set of one partition and one set of the other are possible, an accumulation point of A can be either an interior point or a boundary point of A, etc. Also, we have seen that

(v) $\bar{A} = A \cup \delta A$ and

(vi) $\bar{A} = A \cup \{\text{accumulation points of } A\}$

Unlike (iii) and (iv), the unions (v) and (vi) are in general not disjoint.

$* * *$ *Continuous functions* $* * *$

12.17 Definition. Let (X, τ) and (Y, τ') be topological spaces. A function $f\colon X \to Y$

is called **continuous** if $f^{-1}(O)$ is open for every open set $O \subseteq Y$.

12.18 Remark: Inverse image commutes with arbitrary unions and intersections

$$f^{-1}(\bigcup_{i\in I} S_i) = \bigcup_{i\in I} f^{-1}(S_i) \quad \text{and} \quad f^{-1}(\bigcap_{i\in I} S_i) = \bigcap_{i\in I} f^{-1}(S_i).$$

Therefore, for $f\colon X \to Y$ to be continuous, it suffices that $f^{-1}(O)$ be open for all O in some fixed subbasis of Y. Also,

$$f^{-1}(Y \setminus S) = X \setminus f^{-1}(S).$$

Therefore, $f\colon X \to Y$ is continuous if and only if $f^{-1}(A)$ is closed for every closed set $A \subseteq Y$.

In terms of neighborhoods, a function $f\colon X \to Y$ is continuous, if and only if for every $x \in X$, for every $U \in \mathcal{U}(f(x))$ there exists a $V \in \mathcal{U}(x)$ with $f(V) \subseteq U$. The familiar ε-δ-definition of continuous functions is easily seen to be the specialization to metric spaces of this topological characterization.

12.19 Definition. Let (X,τ) and (Y,τ') be topological spaces. A function $f\colon X \to Y$ is called **open** if $f(O)$ is open for every open set $O \subseteq X$.

A bijective function both open and continuous is called a **homeomorphism**.

A topology τ_1 on X is called **stronger** (or **finer**) than another topology τ_2 on the same set X if $\tau_1 \supseteq \tau_2$ (every τ_2-open set is τ_1-open); τ_2 is then called **weaker** or **coarser** than τ_1. Two trivial topologies exist on every set X: **discrete topology** $\tau = \mathcal{P}(X)$ (the finest topology on X) and **chaotic topology** $\tau = \{\emptyset, X\}$ (the coarsest topology on X).

If τ_1 and τ_2 are two topologies on a set X then τ_1 is stronger than τ_2 iff $\mathrm{id}_X : (X,\tau_1) \to (X,\tau_2)$ is continuous; τ_1 is weaker than τ_2 iff $\mathrm{id}_X : (X,\tau_1) \to (X,\tau_2)$ is open.

$* * *$ *Connectedness* $* * *$

12.20 Definition. A topological space X is **connected**, if, whenenver O_1 and O_2 are open sets with $O_1 \cup O_2 = X$ and $O_1 \cap O_2 = \emptyset$, it follows that $O_1 = \emptyset$ or $O_2 = \emptyset$. A subset Y of X is connected if it is conneced in subspace topology.

12.21 Exercise. If X is connected and $f\colon X \to Y$ continuous, then $f(X)$ is connected.

12.22 Lemma. If X_i is a connected subset of X for every $i \in I$ (I an arbitrary index set) and $\bigcap_{i\in I} X_i \neq \emptyset$ then $\bigcup_{i\in I} X_i$ is connected.

Proof. Easy exercise. $\square$

12.23 Lemma and Definition. The following relation $\sim$ is an equivalence relation on X: $x \sim y$ if and only if there exists a connected subset C of X with $x, y \in C$.

The equivalence classes with respect to $\sim$ are called the **connected components** of X.

From the above definition it is clear that the connected components of X form a partition of X. Also, the component of $x \in X$ is the union of all connected subsets of X containing x, and it is therefore the unique largest connected subset of X containing x.

12.24 Lemma. If Y is a connected subset of X then every set C with $Y \subseteq C \subseteq \overline{Y}$ is connected.

Proof. Exercise. $\square$

12.25 Definition. A topological space X is **locally connected** if every $x \in X$ has a neighborhood basis consisting of connected neighborhoods.

12.26 Lemma. The connected components of a topological space X are closed sets. If every $x \in X$ has a connected neighborhood (in particular, if X is locally connected) then they are also open.

Proof. By the lemma above, the closure of a connected component is again connected and therefore contained in the component. If a point x possesses a connected open neighborhood U_x then the compoment of x (being the union of all connected sets containing x) contains U_x. $\square$

12.27 Definition. A topological space X is **totally disconnected** if it doesn't contain any connected set with more than one element; equivalently, if its connected components are singletons.

$* * *$ *Filters* $* * *$

12.28 Definition. Let X be a set. A **filter** on X is a set $\mathcal{F} \subseteq \mathcal{P}(X)$ with the properties

(1) $\emptyset \notin \mathcal{F}$

(2) If $A, B \in \mathcal{F}$ then $A \cap B \in \mathcal{F}$.

(3) If $A \in \mathcal{F}$ and $X \supseteq C \supseteq A$ then $C \in \mathcal{F}$.

12.29 Definition. Let $\mathcal{F}$ and $\mathcal{G}$ be filters on X. We say that $\mathcal{F}$ is **finer** than $\mathcal{G}$ (or, equivalently, $\mathcal{G}$ is **coarser** than $\mathcal{F}$) if $\mathcal{F} \supseteq \mathcal{G}$.

12.30 Definition. An **ultrafilter** on X is a filter $\mathcal{F}$ with the property:

$$\forall S \subseteq X: \; S \in \mathcal{F} \vee (X \setminus S) \in \mathcal{F}.$$

12.31 Definition. If $\mathcal{F}$ is a filter on X then a subset $\mathcal{F}'$ of $\mathcal{F}$ is called a **filter base** of $\mathcal{F}$ if $\forall F \in \mathcal{F} \; \exists F' \in \mathcal{F}'$ with $F' \subseteq F$.

12.32 Remark: If $\mathcal{F}$ is a filter then $\mathcal{F}' \subseteq \mathcal{F}$ is a filter base of $\mathcal{F}$ if and only if $\mathcal{F}$ consists precisely of all supersets of elements of $\mathcal{F}'$. We can easily give a criterion for a collection of sets $\mathcal{F}' \subseteq \mathcal{P}(X)$ to be the base of a filter on X. The set of supersets of elements of $\mathcal{F}'$ is a filter if and only if $\mathcal{F}'$ has the **finite intersection property**, that is, the intersection of any finite number of sets in $\mathcal{F}'$ is non-empty.

12.33 Lemma. If $\mathcal{F}$ is a filter on X containing neither S nor $X \setminus S$, then there exists a filter $\mathcal{F}_1 \supseteq \mathcal{F} \cup \{S\}$ and a filter $\mathcal{F}_2 \supseteq \mathcal{F} \cup \{(X \setminus S)\}$.

Proof. No $F \in \mathcal{F}$ is contained in S (otherwise S would be in $\mathcal{F}$), and likewise, no $F \in \mathcal{F}$ is contained in $X \setminus S$. Therefore $F \cap (X \setminus S) \neq \emptyset$ for all $F \in \mathcal{F}$ and $F \cap S \neq \emptyset$ for all $F \in \mathcal{F}$. Now take $\mathcal{F} \cup \{S\}$ as a filter base for $\mathcal{F}_1$ and $\mathcal{F} \cup \{(X \setminus S)\}$ as a filter base for $\mathcal{F}_2$. $\square$

12.34 Lemma. A filter is maximal with respect to refinement (i.e., inclusion) if and only if it is an ultrafilter.

Proof. It is clear that no sets can be added to an ultrafilter without violating proprty (1) or (2) in the definition of a filter. Conversely, 12.33 shows that a filter that is not an ultrafilter has a proper refinement. $\square$

12.35 Lemma. For every filter $\mathcal{F}$ on X there exists an ultrafilter on X finer than $\mathcal{F}$. $\mathcal{F}$ is the intersection of all ultrafilters on X finer than $\mathcal{F}$.

Proof. Consider the set S of all filters on X containing $\mathcal{F}$, ordered by inclusion. Since the union of a chain of filters is again a filter, every chain in S has an upper bound in S. By Zorn's Lemma, there exists a maximal element in S, which is an ultrafilter containing $\mathcal{F}$, by 12.34. By 12.33, the intersection of all ultrafilters containing $\mathcal{F}$ contains no other sets than the elements of $\mathcal{F}$. $\square$

∗∗∗ Nets ∗∗∗

12.36 Definition. A **directed set** is a set I With a binary relation $\leq$ such that $\forall i, j, k \in I$

(1) $i \leq i$.

(2) if $i \leq j$ and $j \leq k$ then $i \leq k$.

(3) $\exists n \in I$ with $n \geq i$ and $n \geq j$.

Note that we do not require anti-symmery.

12.37 Definition. A **net** in X is a function from a directed set to X, $\psi: I \to X$, usually written (like a sequence) as a list of values indexed by arguments, $(x_i)_{i \in I}$.

12.38 Definition. Let $\psi: I \to X$, written as $(x_i)_{i \in I}$, be a net in X, J a directed set and and $\varphi: J \to I$ an increasing function that is cofinal in I, that is,

$$\forall i, i' \in I \;\; (i \leq i' \implies \varphi(i) \leq \varphi(i'))$$

$$\forall i \in I \;\; \exists k \in K : \;\; \varphi(k) \geq i.$$

Then the composition of maps $\psi \circ \varphi: J \to X$ is called a **subnet** of $(x_i)_{i \in I}$, and is written $(x_{i_j})_{j \in J}$.

12.39 Definition. Let $(x_i)_{i \in I}$ be a net in X and $S \subseteq X$. We say that (x_i) is **eventually in S** if there exists $n \in I$ such that $x_i \in S$ for all $i \geq n$. We say that (x_i) is **frequently in S**, if for all $n \in I$ there exists $i \in I$ with $i \geq n$ and $x_i \in S$.

12.40 Remark: A set of the form $\{x_i \mid i \geq n\}$ for some $n \in I$ is called a **tail** of the net $(x_i)_{i \in I}$. A net is eventually in a set S if and only if some tail is contained in S; it is frequently in S if and only if all its tails intersect S nontrivially.

12.41 Definition. An **ultranet** in X is a net such that for every subset S of X, the net is eventually in S or eventually in $X \setminus S$.

12.42 Exercise. Let $f: X \to Y$ be any function. If $(x_i)_{i \in I}$ is an ultranet in X then $(f(x_i))_{i \in I}$ is an ultranet in Y. If $\mathcal{F}$ is an ultrafilter on X then $\{f(F) \mid F \in \mathcal{F}\}$ is an ultrafilter on $f(X)$ and $\{S \subseteq Y \mid \exists F \in \mathcal{F} : \;\; f(F) \subseteq S\}$ is an ultrafilter on Y.

∗∗∗ Convergence ∗∗∗

12.43 Definition. Let $\mathcal{F}$ be a filter on X, $x \in X$, and $\mathcal{U}(x)$ the neighborhood filter of x.

$\mathcal{F}$ **converges** to x if and only if $\mathcal{U}(x) \subseteq \mathcal{F}$. In this case, x is called a **limit point** of $\mathcal{F}$.

x is a **cluster point** of $\mathcal{F}$ if and only if $F \cap U \neq \emptyset$ for all $F \in \mathcal{F}$ and all $U \in \mathcal{U}(x)$ (or equivalently, if $x \in \bar{F}$ for all $F \in \mathcal{F}$).

12.44 Proposition. Let $\mathcal{G} \subseteq \mathcal{F}$ be filters on X and $x \in X$.

(1) If $\mathcal{G}$ converges to x then the finer filter $\mathcal{F}$ converges to x.

(2) If x is a cluster point of $\mathcal{F}$ then x is a cluster point of the coarser filter $\mathcal{G}$.

Proof. Follows immediately from the definition of filter convergence and cluster points. $\square$

12.45 Definition. Let $x \in X$ and $\mathcal{U}(x)$ the neighborhood filter of x.

A net in X **converges** to x if and only if for every $U \in \mathcal{U}(x)$, the net is eventually in U. In this case, x is called a **limit point** of the net.

x is a **cluster point** of a net on X if and only if for every $U \in \mathcal{U}(x)$, the net is frequently in U.

12.46 Proposition. Let (x_{n_k}) be a subnet of the net (x_n) on X and $x \in X$. If (x_n) converges to x then the subnet (x_{n_k}) converges to x. If x is a cluster point of the subnet (x_{n_k}) then x is a cluster point of (x_n).

Proof. Follows immediately from the definition of subnet. $\square$

12.47 Proposition. An ultrafilter converges against each of its cluster points. Similarly, an ultranet converges against each of its cluster points.

Proof. Suppose $\mathcal{F}$ is a filter and $x \in X$ such that for all $F \in \mathcal{F}$ and all $U \in \mathcal{U}(x)$, $U \cap F \neq \emptyset$. Then for all $U \in \mathcal{U}(x)$, $(X \setminus U) \notin \mathcal{F}$. If $\mathcal{F}$ is an ultrafilter, $U \in \mathcal{F}$ for all $U \in \mathcal{U}(x)$ follows. The case of nets is similar. $\square$

The following constructions of a net from a filter and a filter from a net often allow to translate statements about filters to statements about nets and vice versa:

12.48 Lemma and Definition. Let $(x_n)_{n \in N}$ be a net on X and $x \in X$. The filter constructed from $(x_n)_{n \in N}$ is defined by taking the set of ends $\{x_n \mid n \geq n_0\}$ for $n_0 \in N$ as a filter basis.

Then the filter constructed from (x_n) converges to x if and only if (x_n) converges to x. Also, x is a cluster point of the filter constructed from (x_n) if and only if x is a cluster point of (x_n).

Proof. Easy exercise. □

12.49 Lemma and Definition. Let $\mathcal{F}$ be a filter on X and $x \in X$. The net constructed from $\mathcal{F}$ is indexed by the set $I = \{(F, y) \mid F \in \mathcal{F}, \quad y \in F\}$ with $(F, y) \geq (F', y') \; :\Longleftrightarrow \; F \subseteq F'$; and $x_{(F,y)} = y$.

Then the net constructed from $\mathcal{F}$ converges to x if and only if $\mathcal{F}$ converges to x. Also, x is a cluster point of the net constructed from $\mathcal{F}$ if and only if x is a cluster point of $\mathcal{F}$.

Proof. Easy exercise. □

12.50 Exercise. Let $\mathcal{F}$ be a filter on X and $x \in X$. For each $F \in \mathcal{F}$ choose $x_F \in F$. Does the net $(x_F)_{F \in \mathcal{F}}$ (indexed by $\mathcal{F}$ directed by $F' \geq F \; :\Longleftrightarrow \; F' \subseteq F$), also satisfy the equivalences of 12.49?

12.51 Remark: For a filter $\mathcal{F}$ to converge to $x \in X$, it suffices that $\mathcal{F}$ contains, for a fixed subbasis S of the topology, every $Y \in S$ with $x \in Y$. Similarly, for a net to converge to x, it suffices that it is eventually in Y for every $Y \in S$ with $x \in Y$.

Proof. Easy exercise. □

$* * *$ *Compactness* $* * *$

12.52 Definition. Let X be a topological space and $Y \subseteq X$. An **open cover** of Y is a set $\mathcal{C}$ of open sets such that $Y \subseteq \bigcup_{O \in \mathcal{C}} O$. Y is **compact** if every open cover of Y admits a finite subcover, that is, there exist $O_1, \ldots, O_n \in \mathcal{C}$ with $Y \subseteq O_1 \cup \ldots \cup O_n$.

Be aware that many authors require compact sets to be Hausdorff, and call our notion of compact "quasi-compact".

12.53 Exercise. If X is compact and $f : X \to Y$ continuous, then $f(X)$ is compact.

12.54 Theorem. Let X be a topoological space, and S a subbasis of the topology. The following are equivalent:

(1) X is compact, i.e., every open cover of X has a finite subcover.

(2) Every cover of X consisting of elements of S has a finite subcover.

(3) Every ultrafilter on X converges to some $x \in X$.

(4) Every filter on X has a cluster point $x \in X$.

Proof. ($1 \Rightarrow 2$) a fortiori.

($2 \Rightarrow 3$) Suppose the ultrafilter $\mathcal{U}$ doesn't converge. For every $x \in X$ choose $U_x \in S$ with $x \in U_x$ and $U_x \notin \mathcal{U}$ (possible by 12.51) and let $A_x = X \setminus U_x$. Then $A_x \in \mathcal{U}$. Also, $\{U_x \mid x \in X\}$ covers X so there exists a finite set $Y \subseteq X$ with $\bigcup_{x\in Y} U_x = X$. Therefore $\emptyset = \bigcap_{x\in Y} A_x \in \mathcal{U}$, a contradiction.

($3 \Rightarrow 4$) By 12.35, every filter $\mathcal{F}$ on X can be refined to an ultrafilter. This ultrafilter converges to some $x \in X$ and then x is a cluster point of $\mathcal{F}$ by 12.44.

($4 \Rightarrow 1$) Suppose $\mathcal{C}$ is an open cover of X that has no finite subcover. Then we may use $\{X \setminus O \mid O \in \mathcal{C}\}$ as base for a filter $\mathcal{F}$ on X. Let $x \in X$ be a cluster point of $\mathcal{F}$ and $O_x \in \mathcal{C}$ with $x \in O_x$. Then $F \cap O_x \neq \emptyset$ for all $F \in \mathcal{F}$. But $(X \setminus O_x) \in \mathcal{F}$, a contradiction. $\square$

12.55 Corollary. Let X be a topologial space. Let $\mathcal{B} \subseteq \mathcal{P}(X)$ be a set of closed sets such that every closed subset of X is representable as an arbitrary intersection of finite unions of elements of $\mathcal{B}$ (or, equivalently, such that $\mathcal{S} = \{(X \setminus A) \mid A \in \mathcal{B}\}$ is a subbasis of the topology on X). Then the following are equivalent.

(1) X is compact.

(1') For every set $\mathcal{A} \subseteq \mathcal{P}(X)$ of closed subsets of X it is true that: if $\bigcap_{A\in\mathcal{A}} A = \emptyset$ then there exists a finite subset $\{A_1, \ldots, A_n\} \subseteq \mathcal{A}$ with $\bigcap_{1\le i\le n} A_i = \emptyset$.

(2') Like (1'), but restricted to sets of closed sets $\mathcal{A} \subseteq \mathcal{B}$.

(3') Every ultranet in X converges to some $x \in X$.

(4') Every net in X has a cluster point $x \in X$.

Proof. ($1 \Leftrightarrow 1'$) and ($2 \Leftrightarrow 2'$) by de Morgan. ($3 \Leftrightarrow 3'$) and ($4 \Leftrightarrow 4'$) by 12.48 and 12.49. $\square$

12.56 Exercise. If X is Hausdorff, then we can separate disjoint compact sets C_1, C_2 by open sets, i.e., there are open sets O_1, O_2 such that $C_1 \subseteq O_1$, $C_2 \subseteq O_2$ and $O_1 \cap O_2 = \emptyset$. (First show that we can separate a compact set C from a point $x \in X \setminus C$ by open sets.)

12.57 Exercise.

(i) Every closed subset of a compact space is compact.

(ii) If X is Hausdorff, then every compact subset of X is closed.

$***$ *Product topology* $***$

12.58 Definition. For $i \in I$ (an arbitrary index set) let X_i be a topological space. **Product topology** on the cartesian product $\prod_{i\in I} X_i$ is defined by a subbasis consisting of all sets of the form

$$S(j, O_j) = \{(x_i)_{i\in I} \in \prod_{i\in I} X_i \mid x_j \in O_j\},$$

for some $j \in I$, and some O_j open $\subseteq X_j$. (Equivalently, the sets O_j could be restriced to members of a given basis or subbasis of the topology of X_j.)

Remark: the finer topology on $\prod_{i\in I} X_i$ given by the basis

$$\mathcal{B} = \{\prod_{i\in I} O_i \mid \forall i\, O_i \text{ open } \subseteq X_i\}$$

is called **box topology**.

Note that the projections $p_j: (\prod_{i\in I} X_i) \to X_j$, $p_j((x_i)_{i\in I}) = x_j$, are continuous, both for product topology and for box topology.

12.59 Proposition. A net $(x_\lambda)_{\lambda\in\Lambda}$ in $X = \prod_{i\in I} X_i$ converges to $y = (y_i)_{i\in I}$ in product topology, if and only if for every $i \in I$, its projection to X_i, $(p_i(x_\lambda))_{\lambda\in\Lambda}$ converges to y_i in X_i.

Proof. Easy exercise. □

12.60 Theorem (Tychonoff). $X = \prod_{i\in I} X_i$ (with product topology) is compact if and only if each X_i is compact.

Proof. Easy direction: if $\prod_{i\in I} X_i$ is compact, then for each i, X_i is compact as the image of $\prod_{i\in I} X_i$ under the projection onto the i-th coordinate, which is continuous. Conversely, to show compactness of $X = \prod_{i\in I} X_i$, consider an ultranet on X. The projection to the i-the coordinate is an ultranet on X_i, which converges, since X_i is compact. As all coordinates of the ultranet converge, the ultranet itself converges. □

We give another proof of Tychonoff's theorem using a different criterion for compactness.

Proof. Easy direction: if $\prod_{i\in I} X_i$ is compact and $\mathcal{C}$ is an open cover of X_i, then $\{S(i, O) \mid O \in \mathcal{C}\}$ is an open cover of X, which has a finite subcover $S(i, O_1), \ldots, S(i, O_n)$. Clearly, $O_1, \ldots, O_n$ cover X_i and constitute a finite subcover of $\mathcal{C}$.

Now assuming compactness of each X_i, to show compactness of $X = \prod_{i\in I} X_i$, consider a cover $\mathcal{C}$ by subbasis elements $S(i, O)$. There must be some coordinate $j \in I$ such that the open sets O occurring in sets $S(j, O) \in \mathcal{C}$ cover X_j. (Otherwise, by the axiom of choice, there would be a point $(x_i)_{i\in I}$ such that for all i, x_i is in none of the sets O with $S(i, O) \in \mathcal{C}$, and therefore $(x_i)_{i \in I}$ is not covered by $\mathcal{C}$.) As X_j is compact, there is a finite cover of X_j by open sets $O_1, \ldots O_n$ with $S(j, O_k) \in \mathcal{C}$. Clearly then $S(j, O_1)$, …, $S(j, O_n)$ cover X. $\square$