8.4. **Noether Normalisation.**

Theorem (Noether normalisation Lemma)**.** *Let k be a field and A a finitely generated k-algebra; then there are elements $z_1, \dots, z_m \in A$ such that $B = k[z_1, \dots, z_m]$ is isomorphic to a polynomial ring in m-variables and A is integral over B. In fact A is a finitely generated B-module.*

Proof. Suppose A is generated by $x_1, \dots, x_n$ over k. If the x_i are algebraically independent over k then we may take $m = n$ and $B = A$.

Otherwise, there is a non-trivial polynomial $f = \sum_{\mathbf{i}} \alpha_{\mathbf{i}} t^{\mathbf{i}}$ in $k[t_1, \dots, t_n]$ such that $f(x_1, \dots, x_n) = 0$. Given positive integers $a_1, a_2, \dots, a_{n-1}$ we may define $y_i = x_i - x_n^{a_i}$ for $i < n$. Substituting into f and writing $\mathbf{a} = (a_i)$ (with $a_n = 1$) we obtain

$$\sum_{\mathbf{i}} \alpha_{\mathbf{i}} x_1^{\mathbf{i}\cdot\mathbf{a}} + g(x_l, y_2, \dots, y_n) = 0$$

for some polynomial g containing no monomials purely in x_n. Now if $a_i = d^{n-i}$ for some large positive integer d — say $d > \deg f$ — then we may arrange for $\mathbf{i}\cdot\mathbf{a} \neq \mathbf{j}\cdot\mathbf{a}$ whenever $\mathbf{i} \neq \mathbf{j}$ and $\alpha_{\mathbf{i}}, \alpha_{\mathbf{j}}$ are both non-zero. Thus x_n is integral over $k[y_1, \dots, y_{n-1}]$. But $x_1, \dots, x_{n-1}]$ are manifestly integral over $k[y_1, \dots, y_{n-1}, x_n]$ so by transitivity of integral extensions A is integral over $k[y_1, \dots, y_{n-1}]$. By induction on the number of generators of A we may find $z_1, \dots, z_m \in k[y_2, \dots, y_n]$ such that $z_1, \dots, z_m$ are algebraically independent over k and $k[y_1, \dots, y_{n-1}]$ is integral over $k[z_1, \dots, z_m]$. By transitivity of integral extensions again, we get A is integral over $k[z_1, \dots, z_m]$ as required. □

Remarks.

(1) If k is an infinite we can use a linear change of variables instead of the one described: this is an older (and sometimes more useful) result.

(2) Geometrically the theorem says that if A is a finitely generated k-algebra then there is finite map from Spec(A) to affine m-space=Spec(B).

Corollary (Weak Nullstellensatz)**.** *If A is a finitely generated k-algebra and a field then A is a finite algebraic extension of k.*

Proof. By Noether Normalisation there is a subring B of A such that $B = k[z_1, \dots, z_m]$ is free on m-generators and A is integral over B.

Now $\text{K-dim}\, A = \text{K-dim}\, B$ since A is integral over B. But since A is a field $\text{K-dim}\, A = 0$. Thus $\text{K-dim}\, B = 0$. It follows that $m = 0$ since otherwise $0 < (z_1)$ is a chain of prime ideals in Spec(B) of length 1.

So $B = k$ and A is integral over k as required. □

Notice that the argument actually shows that if A is a finitely generated k-algebra there is an m such that $\text{K-dim}\, A = \text{K-dim}\, k[x_1, \dots, x_m]$. It is easy to see that $\text{K-dim}\, k[x_1, \dots, x_m] \geq m$. We will see late that it is actually m.

8.5. **Valuations.**

Definition. Let A be an integral domain. We say that A is a valuation ring if for every $x \in Q(A)\backslash 0$ either $x \in A$ or $x^{-1} \in A$.

We will now try to show that if A is an integral domain then the integral closure of A in its field of fractions $Q(A)$ is the interection of all the valuation rings of $Q(A)$ containing A. We'll also use valuation rings to give another proof of the weak Nullstellensatz.

Examples.

(1) $\mathbb{Z}$ is not a valuation ring, e.g. $2/3, 3/2 \notin \mathbb{Z}$.
(2) $\mathbb{Z}_{(p)}$ is a valuation ring. (Notice $\mathbb{Z} = \cap_p \mathbb{Z}_{(p)}$).

Lemma. *If A is a valuation ring, then*

(i) A is a local ring.
(ii) Every ring that contains A and is contained in $Q(A)$ is a valuation ring.
(iii) A is integrally closed.

Proof.

(i) We want to show that the set of non-units of A is an ideal. For this it suffices to show that if x and y are not units in A then $x+y$ is not a unit in A. WLOG x, y are both non-zero, so one of $x^{-1}y$ or $y^{-1}x$ is in A. WLOG $x^{-1}y$. Then $x + y = (1 + x^{-1}y)x$. Since x is not a unit it follows that $x + y$ is not a unit.

(ii) Is clear.

(iii) Suppose that x is in $Q(A)$ and is integral over A but is not in A. Then x^{-1} is in A. Moreover, $x^n + a_1x^{n-1} + \cdots + a_n = 0$ for some a_i in A.

But we may deduce from this equation that

$$x = -(a_1 + a_2x^{-1} + \cdots + a_nx^{1-n}).$$

Since the RHS is in A so is the LHS, a contradicton □

Now we prove a technical lemma that we will use later.

Lemma. *If A is a local integral domain with maximal ideal $\mathfrak{m}$ and $x \in Q(A)\backslash 0$ then either $(\mathfrak{m}) \lhd A[x]$ is a proper ideal or $(\mathfrak{m}) \lhd A[x^{-1}]$ is a proper ideal.*

Proof. Suppose not, then choose $m + n$ to be minimal such that we may find $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathfrak{m}$ with $\sum_{i=0}^n a_ix^i = 1 = \sum_{j=0}^m b_ix^{-i}$. Without loss of generality, $0 < m \le n$.

Now $(1 - b_0) = \sum_{i=1}^m b_ix^{-i} \in A^\times$. So

$$x^n = x^n(1 - b_0)^{-1}(\sum_{i=1}^m b_ix^{-i}) \in \sum_{i=0}^{n-1} \mathfrak{m}x^i$$

so there are $a'_0, \ldots, a'_{n-1} \in \mathfrak{m}$ with $\sum_{i=0}^{n-1} a'_ix^i = 1$, giving the desired contradiction. □

Now we consider the following set-up: Suppose that A is an integral domain and that K is an algebraically closed field and consider the set X of pairs (B, f) with B a subring of $Q(A)$ containing A and $f: B \to K$ a ring homomorphism.

We make X into a poset by $(B, f) \le (C, g)$ precisely if $B \subset C$ and $g|_B = f$. It is easy to check that the poset $(X, \le)$ is chain complete and so has maximal elements.

Theorem. *If (B, f) is a maximal element of $(X, \le)$ then B is a valuation ring in $Q(A)$ with maximal ideal* $\ker f$.

Proof. First we show that $\ker f$ contains all the non-units in B: certainly $f(B)$ is a subring of K and so an integral domain, so $\ker f$ is prime. Letting $S = B \backslash \ker f$, we may extend f to a ring homomorphism $f_S: B_S \to K_S = K$. By maximality of the pair (B, f) we see that necessarily $B_S = B$ and so every element of S is a unit in B and $\ker f$ is the unique maximal ideal in B.

Now we want to show that if $x \in Q(A)$ then either $x \in B$ or $x^{-1} \in B$. By replacing x by x^{-1} if necessary and applying the lemma we may assume that $(\ker f) \lhd B[x]$ is a proper ideal.

Let $\mathfrak{m}$ be an element of $\operatorname{maxSpec}(B[x])$ containing $\ker f$. Since $x \in Q(B) = Q(A)$, x is algebraic over $Q(A)$ so $B[x]/\mathfrak{m}$ is algebraic over $B/\ker f$, so as K is algebraically closed, we may extend $\overline{f}\colon B/\ker f \to K$ to $\overline{g}\colon B[x]/\mathfrak{m} \to K$. Then $\overline{g}$ induces $g\colon B[x] \to K$ extending f and so $x \in B$. □

Corollary. *If A is an integral domain then its integral closure in $Q(A)$ is the intersection of all valuation rings in $Q(A)$ containing A.*

Proof. Since valuation rings are all integrally closed, the integral closure of A is $Q(A)$ is contained in every valuation ring in $Q(A)$ containing A so we just need to show that if x is not in the integral closure of A then there is such a valuation ring not containing it.

So suppose x is $Q(A)$ but not integral over A. Let $B = A[x^{-1}]$. Then $x \notin B$. So x^{-1} is not a unit in B and there is a maximal ideal $\mathfrak{m}$ of B containing x^{-1}. Let K be the algebraic closure of $B/\mathfrak{m}$ then there is a natural ring homomorphism f from B to K with kernel $\mathfrak{m}$. Picking a maximal element (C, g) of X above (B, f), we see that C is a valuation ring in $Q(A)$ and $g(x^{-1}) = 0$ so x is not in C. □

We can now reprove the weak Nullstellensatz.

Corollary. *Suppose $A \subset B$ are integral domains and B is a finitely generated A-algebra. For each $b \in B\backslash 0$, there exists $a \in A\backslash 0$ such that any homomorphism f from A to an algebraically closed field K with $f(a) \neq 0$ may be extended to a homomorphism g from B to K with $g(b) \neq 0$.*

In particular, if $K = \overline{k}$ and B is a finitely generated k-algebra and a field, then B is isomorphic to a finite algebraic extension of k.

Proof. By inducting on the number of generators of B as an A-algebra we can assume $B = A[x]$. Then either x is algebraic or trancendental over A. In the latter case, we may write $b = a_0x^n + \cdots + a_n$, with $a_i \in A$ and $a_0 \neq 0$. Let $a = a_0$. Since K is infinite, whenever $f\colon A \to K$ is a ring homomorphism with $f(a) \neq 0$, there is a $\alpha \in K$ that is not a root of $f(a_0)t^n + \cdots + f(a_n)$. We can define $g\colon B \to K$ to be the extension of f that sends x to α so $g(b) \neq 0$ as required.

If x is algebraic over A, then so is b since the set of algebraic elements of $Q(B)$ over $Q(A)$ is a field. So there are $a_0, \ldots, a_n$ in A and $a'_0, \ldots, a'_m$ in A such that $\sum_{i=0}^n a_i x^i = 0$ and $\sum_{j=0}^m a'_j b^j = 0$.

Let $a = a_n a'_0$ so x and b^{-1} are both integral over A_a, and suppose that f is a homomorphism $A \to K$ such that $f(a) \neq 0$. So f extends to $f_a\colon A_a \to K$. But now by our theorem we may extend f_a to a map $h\colon C \to K$ for some valution ring C in $Q(B)$. Since x is integral over A_u, C contains x and so also B and we can define $g = h|_B$.

Finally, as b^{-1} is integral over A_u it must live in C, thus b is a unit in C and $g(b) = h(b) \neq 0$ as required.

For the last part, take $v = 1$, $A = k$, □

9. Dedekind domains

9.1. Discrete valuation rings.

Definition. If K is a field then a *discrete valuation* on K is a surjective group homomorphism $v\colon K^\times(\mathbb{Z},+)$ such that $v(x+y) \geq \min(v(x), v(y)$ for all $x, y \in K^\times$. [By convention $v(0) := \infty \geq n$ for all $n \in \mathbb{Z}$]. Then $K_v = \{x \in K \mid v(x) \geq 0\}$ is a subring of K, the *valuation ring* of v.

Notice if $x \in K^\times$ either $v(x) \geq 0$ or $v(x^{-1} \geq 0$ so K_v is a valuation ring.

Examples.

(1) If $K = \mathbb{Q}$ and $p \in \mathbb{Z}$ is prime, $v_p\colon \mathbb{A}^\times \to \mathbb{Z}$; $p^a \frac{x}{y} \mapsto a$ (for x, y coprime of p) is a discrete valuation and $K_{v_p} = \mathbb{Z}_{(p)}$.

(2) If $K = \mathbb{C}(x)$ and $\lambda \in \mathbb{C}$, let $v_\lambda\colon \mathbb{C}(x)^\times \to \mathbb{Z}$; $(x-\lambda)^a \frac{f(x)}{g(x)} \to a$ (for $f(\lambda), g(\lambda) \neq 0$). Then $K_{v_\lambda} = \mathbb{C}[x]_{(x-\lambda)}$.

Exercise. Show that these are all the discrete valuations of $\mathbb{Q}$ and $\mathbb{C}(x)$.

Definition. An integral domain A is a *discrete valuation ring* (DVR) if there is a discrete valuation v of $Q(A)$ such that $Q(A)_v = A$.

Since a DVR is a valuation ring, it must be local and it is easy to see that the unique maximal ideal of A is $\mathfrak{m} = \{x \in Q(A) \mid v(x) \geq 1\}$.

Notice too that if $v(x) = v(y)$ then $v(xy^{-1}) = 0$ so xy^{-1} is a unit in A and $(x) = (y)$. Given any non-zero ideal I in A. If $x \in I$ has least value amongst elements of I then $v(yx^{-1}) \geq 0$ for all $y \in I$ so $(x) \subset I \subset (x)$. It follows that in a DVR every ideal is principal and of the from $\{x \in A \mid v(x) \geq k\}$. Thus DVRs are Noetherian and have Krull dimension 1; the only primes are (0) and $\mathfrak{m}$.

Since v is surjective, there is $x \in A$ with $v(x) = 1$. Then $(m) = (x)$ any every ideal is of the from (x^k). Also we never have $\mathfrak{m}^k = \mathfrak{m}^{k+1}$, since $v(x^k) = k < k+1 = v(x^{k+1})$.

There are many ways to characterise DVRs:

Lemma. *Let A be a Noetherian local integral domain of Krull dimension* 1 *with maximal ideal $\mathfrak{m}$. The following are equivalent:*

(i) *A is a DVR;*
(ii) *A is integrally closed;*
(iii) *$\mathfrak{m}$ is principal;*
(iv) *There is $x \in \mathfrak{m}$ such that every non-zero ideal is of the form (x^k) for some $k \geq 0$;*
(v) $\mathrm{Frac}(A) = Cart(A)$*; that is A is a Dedekind domain;*
(vi) $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

Proof.

$(i) \implies (ii)$: DVRs are valuation rings and valuation rings are integrally closed

$(ii) \implies (iii)$: we use the fact that x is integral over A if and only if there is an $A[x]$-module M such that $\mathrm{Ann}_{A[x]}(M) = 0$ and M is f.g. over A.

Let $x \in \mathfrak{m}$ non-zero. Then $A/(x)$ has a unique prime ideal $\overline{\mathfrak{m}} = \mathfrak{m}/(x)$. As $A/(x)$ is Noetherian, $\overline{\mathfrak{m}}$ is nilpotent so there is a least n such that $\overline{m}^n = 0$. Pick $y \in \mathfrak{m}^{n-1} \backslash (x)$. Then $yx^{-1} \in Q(A) \backslash A$ so is not integral over A by assumption. Thus $yx^{-1}\mathfrak{m} \not\subset \mathfrak{m}$ as $\mathfrak{m}$ is finitely generated over A so cannot be an $A[yx^{-1}]$-module.

But $yx^{-1}\mathfrak{m} \subset A$ as $y\mathfrak{m} \subset \mathfrak{m}^n \subset (x)$. So $yx^{-1}\mathfrak{m} = A$ and $\mathfrak{m} \in \text{Cart}(A)$ so is principal ($Pic(A) = 0$ since A is local).

$(iii) \implies (iv)$: let $x \in A$ generate $\mathfrak{m}$ and $0 \neq I \lhd A$. There is n largest such that $\mathfrak{m}^n \subset I$ as again $\mathfrak{m}/I$ is nilpotent in A/I. Then there is $y \in I \backslash \mathfrak{m}^{n+1}$ and $y = ax^n$ some $a \in A \backslash \mathfrak{m} = A^\times$. So $x^n = a^{-1}y \in I$ and $(x^n) \subset I \subset (x^n)$.

$(iv) \implies (i)$: let $v\colon A\backslash 0 \to \mathbb{N}_0$ be given by $v(a) = k$ if $(a) = (x^k)$. Nakayma's Lemma gives that $(x^k) supsetneq (x^{k+1})$ for all k so v is well-defined. It is easy to check that $v(ab) = v(a)v(b)$ for all a, b and $v(a + b) \geq \min(v(a), v(b))$ since if $(a) = (x^k)$ and $(b) = (x^l)$ then $(a + b) \subset (x^{\min(k,l)})$.

Next, we extend v to a map from $Q(A)\backslash 0$ to $\mathbb{Z}$ by $v(a/b) = v(a) - v(b)$. It is then straightforward to check v is a well-defined discrete valuation on $Q(A)$ and $Q(A)_v = A$.

$(iii) \iff (vi)$ follows from Nakayama's Lemma

Finally we see that $(v) \iff$ every fractional ideal is principal (since $\text{Pic}(A)$ must be 0 when A is local). Now $(v) \implies (iii)$ and $(iv) \implies (v)$ are clear □

Proposition. *Let A be a local integral domain with maximal ideal $\mathfrak{m} \neq 0$. Then A is a DVR or a field if and only if $\text{Frac}(A) = \text{Cart}(A)$. In particular local Dedekind domains are Noetherian of Krull dimension 1.*

Proof. The forwards implication follows from the lemma. For the reverse implication it suffices to handle the last sentence since then it follows from the lemma.

So suppose $\text{Frac}(A) = \text{Cart}(A)$. Since line bundles are finitely generated and every ideal is a fractional ideal and so a line bundle we see A is Noetherian.

Suppose $P \in \text{Spec}(A)\backslash\{\mathfrak{m}, 0\}$ [ie $KdimA > 1$]. Then $\mathfrak{m}^{-1}P \subsetneq A$ as $P \subsetneq \mathfrak{m}$. But $\mathfrak{m}(\mathfrak{m}^{-1}P) = P$ so as P is prime and $\mathfrak{m} \not\subset P$, $\mathfrak{m}^{-1}P \subset P$. Then $P \subset \mathfrak{m}P$ contradicting Nakayama's Lemma. □

9.2. **Dedekind domains.** We now drop the locality hypotheses of the previous section.

Theorem. *Suppose A is a Noetherian domain of Krull dimension 1. The following are equivalent:*

(i) A is a Dedekind domain
(ii) A is integrally closed
(iii) A_P is a DVR for all $P \in \text{Spec}(A)$ non-zero.

Proof. $(ii) \iff (iii)$ follows from the facts that for A to be integrally closed is a local property and that local integrally closed Noetherian domains of Krull dimension 1 are DVRs.

For $(i) \iff (iii)$ it will suffice to prove that to be a Dedekind domain is a local property. That is $\text{Frac}(A_P) = \text{Cart}(A_P)$ for all $P \in \text{Spec}(A)\backslash 0 \iff \text{Frac}(A) = \text{Cart}(A)$.

Suppose $I \in \text{Frac}(A)$. Let $J = \{x \in Q(A) \mid xI \subset A\}$. So $IJ \subset A$ and $IJ = A$ precisely if $I \in \text{Cart}(A)$.

Then for each $P \in \text{Spec}(A)$, $x \in Q(A)$ we have $xI_P \subset A_P$ if and only if there is $s \in A\backslash P$ such that $sxI \subset A$ if and only if $x \in J_P$. So $J_P = \{x \in Q(A) \mid xI_P \subset A_P\}$.

Now $I \in Cart(A)$ if and only if $IJ = A$ if and only if $(IJ)_P = I_P J_P = A_P$ for each $P \in \text{Spec}(A)$ if and only if $I_P \in \text{Cart}(A_P)$ for all $P \in \text{Spec}(A)$ as required. □

Suppose now that A is a Dedekind domain. A is Noetherian since ideals are all line bundles and so finitely generated. Moreover K-dim $A \leq 1$ since if $P \in \text{Spec}(A)$ then A_P is a local Dedekind domain so has Krull dimension at most 1.

Suppose that I is a non-zero ideal in A then for each $P \in \text{Spec}(A)\backslash 0$ we have A_P is a DVR and $I_P = (P_P)^{k_P}$ for some $k_p \geq 0$. Moreover, if $k_P > 0$ then $I \subset P$. But A/I is Noetherian of Krull dimension 0 so has only finitely many non-zero prime ideals (minimal primes). So $k_P = 0$ for all but finitely many primes.

Now we may define $J = \prod_{P \in \text{Spec}(A)\backslash 0} P^{k_P}$ a finite product since all but finitely many terms are 1. But by contruction $J_P = I_P$ for all $P \in \text{Spec}(A)$ and so $I = J$. Thus we have proven the following result.

Theorem. *If A is a Dedekind domain then every non-zero ideal may be expressed uniquely as $\prod_{P \in \text{Spec}(A)\backslash 0} P^{k_P}$ with $k_P \in \mathbb{N}_0$ and $k_P = 0$ for all but finitely many P.*

Exercise. Show that we may extend to Frac(A) is the free abelian group generated by $\text{Spec}(A)\backslash 0$ whenever A is a Dedekind domain.

We'll close this section with one final characterisation of Dedekind domains

Theorem. *If A is a Noetherian integral domain then the following are equivalent:*

(i) every finitely generated torsion free A-module is projective;
(ii) if M is a finitely generated A-module and X is a finitely generated projective A-module and $\pi \in \text{Hom}_A(X, M)$ is surjective then $\ker \pi$ is projective;
(iii) A is a Dedekind domain

Part (ii) is sometimes phrased as A has *global dimension* at most 1.

Proof.

$(i) \implies (ii)$: since X is finitely generated projective and so torsion free, $\ker \pi$ is finitely generated (as A is Noetherian) and torsion free. So $\ker \pi$ is projective by assumption.

$(ii) \implies (iii)$: let $0 \neq I$ be a fractional ideal in A then there is a non-zero $f \in A$ such that fI is an ideal in A. Let $\pi\colon A \to A/fI$ be the natural projection so $\ker \pi = fI$. By assumption $\ker \pi$ is projective. But $Q(A) \otimes_A fI \cong Q(A)$ so fI is a line bundle. Thus $fI \in Cart(A)$. But $f^{-1} \in \text{Cart}(A)$ so I is a Cartier divisor.

$(iii) \implies (i)$: let M be a finitely generated torsion free A-module. We proceed by induction on $\text{rk}_M((0))$.

If $\text{rk}_M((0)) = 0$ then $M = 0$ as so projective since M is torsion free.

Suppose $\text{rk}_M((0)) = n + 1$. Then $Q(A) \otimes_A M \cong Q(A)^{n+1}$. Let $\pi\colon Q(A)^{n+1} \to Q(A)$ project onto the first coordinate. Then consider the image M_0 of M under the composite $M \to Q(A) \otimes_A M \to Q(A)^{n+1} \xrightarrow{\pi} Q(A)$. Since M is finitely generated M_0 is also. Thus M_0 is a fractional ideal and so a line bundle by assumption.

In particlar M_0 is projective and so the projection map $M \to M_0$ splits and $M \cong M_0 \oplus M'$ for some finitely generated torsion free A-module M' with $rk_{M'}((0)) = n$. By the induction hypothesis M' is projective and we're done. $\square$