3. Noether Normalization and Applications

Integral extension of a ring means adjoining roots of monic polynomials over the ring. This is an important tool for studying affine rings, and it is used in many places, for example, in dimension theory, ring normalization and primary decomposition. Integral extensions are closely related to finite maps which, geometrically, can be thought of as projections with finite fibres plus some algebraic conditions. We shall give a constructive introduction with explicit algorithms to these subjects.

3.1 Finite and Integral Extensions

This section contains the basic algebraic theory of finite and algebraic extensions and their relationship. Moreover, important criteria for integral dependence (Proposition 3.1.3) and finiteness (Proposition 3.1.5) are proven.

Definition 3.1.1. Let $A \subset B$ be rings.

(1) $b \in B$ is called *integral* over A if there is a monic polynomial $f \in A[x]$ satisfying $f(b) = 0$, that is, b satisfies a relation of degree p,

$$b^p + a_1 b^{p-1} + \cdots + a_p = 0, \quad a_i \in A\ ,$$

for some $p > 0$.

(2) B is called *integral over* A or an *integral extension* of A if every $b \in B$ is integral over A.

(3) B is called a *finite extension* of A if B is a finitely generated A–module.

(4) If $\varphi : A \to B$ is a ring map then φ is called an *integral*, respectively *finite, extension* if this holds for the subring $\varphi(A) \subset B$.

If there is no doubt about φ, we say also, in this situation, that B is integral, respectively finite, over A. Often we omit φ in the notation, for example we write IM instead of $\varphi(I)M$ if $I \subset A$ is an ideal and M a B–module.

Proposition 3.1.2. *Let A, B be rings.*

(1) If $\varphi : A \to B$ is a finite extension, then it is integral. More generally, if $I \subset A$ is an ideal and M a finitely generated B–module then any $b \in B$ with $bM \subset IM$ satisfies a relation

$$b^p + a_1 b^{p-1} + \cdots + a_p = 0\,, \qquad a_i \in I^i \subset A\,.$$

(2) If B is a finitely generated A–algebra of the form $B = A[b_1, \ldots, b_n]$ with $b_i \in B$ integral over A then B is finite over A.

Proof. (1) Replacing A by the image of A, we may assume that $A \subset B$. Any $b \in B$ defines an endomorphism of the finitely generated A–module B. The characteristic polynomial of this endomorphism defines an integral relation for b, by the *Cayley–Hamilton Theorem* (this is sometimes called the "determinantal trick").

In concrete terms, let $b_1, \ldots, b_k$ be a system of generators for B as A–module, then $b \cdot b_i = \sum_{j=1}^{k} a_{ij} b_j$, $1 \leq i \leq k$, for suitable $a_{ij} \in A$. This implies

$$\big(b \cdot E_k - (a_{ij})\big) \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} = 0\,,$$

therefore, by Cramer's rule, $\det\big(b \cdot E_k - (a_{ij})\big) \cdot b_i = 0$ for $i = 1, \ldots, k$.[1] But, since $1 = \sum_i e_i b_i \in B$ for suitable $e_1, \ldots, e_k$, we obtain $\det\big(bE_k - (a_{ij})\big) = 0$, which is the required integral relation for b.

In the general case, let $b_1, \ldots, b_k$ be a system of generators of M as A–module. Then we can choose the a_{ij} from I and it follows that the coefficient of b^{k-i} in $\det(bE_k - \big(a_{ij})\big)$ is a sum of $i \times i$–minors of (a_{ij}) and, therefore, contained in I^i.

(2) We proceed by induction on n. If b_1 satisfies an integral relation of degree p, then b_1^p and hence, any power b_1^q, $q \geq p$, can be expressed as an A–linear combination of $b_1^0, \ldots, b_1^{p-1}$. That is, the A–module $B = A[b_1]$ is generated by $b_1^0, \ldots, b_1^{p-1}$, in particular, it is finite over A.

For $n > 1$ we may assume, by induction, that $A[b_1, \ldots, b_{n-1}]$ is finite over A. Since taking finite extension is clearly transitive, $(A[b_1, \ldots b_{n-1}])[b_n]$ is finite over A. □

Let K be a field, $I \subset K[x] := K[x_1, \ldots, x_n]$ an ideal and $f_1, \ldots, f_k \in K[x]$. The residue classes $\bar{f}_i = f_i \bmod I$ generate a subring

$$A := K[\bar{f}_1, \ldots, \bar{f}_k] \subset B := K[x]/I\,.$$

We want to check whether a given $b \in K[x]$ is integral over $K[f_1, \ldots, f_k] \bmod I$, that is, whether $\bar{b}$ is integral over A.

[1] Here E_n denotes the $n \times n$ unit matrix.

The following two results are the basis for an algorithm to check for integral dependence respectively finiteness.

Proposition 3.1.3 (Criterion for integral dependence).
Let $b, f_1, \dots, f_k \in K[x]$, $I = \langle g_1, \dots, g_s \rangle \subset K[x]$ an ideal and $t, y_1, \dots, y_k$ new variables. Consider the ideal

$$M = \langle t - b,\, y_1 - f_1, \dots,\, y_k - f_k,\, g_1, \dots, g_s \rangle \subset K[x_1, \dots, x_n, t, y_1, \dots, y_k]\,.$$

Let $>$ be an ordering on $K[x, t, y]$ with $x \gg t \gg y$,[2] *and let G be a standard basis of M with respect to this ordering.*

Then b is integral over $K[f] = K[f_1, \dots, f_k]$ mod I if and only if G contains an element g with leading monomial $\mathrm{LM}(g) = t^p$ for some $p > 0$. Moreover, any such g defines an integral relation for b over $K[f]$ mod I.

Proof. If $\mathrm{LM}(g) = t^p$ then g must have the form

$$g(t, y) = a_0 t^p + a_1(y) t^{p-1} + \dots + a_p(y) \in K[t, y], \quad a_0 \in K \setminus \{0\}\,.$$

We may assume that $a_0 = 1$. Since $g \in M$ we have $g(b, f) \in I$. Thus, g defines an integral relation for b over $K[f]$ mod I.

Conversely, if b is integral, then there exists a $g \in K[t, y]$ as above. By Taylor's formula, $g(t, y) = g(b, f) + b_0 \cdot (t - b) + \sum_{i=1}^{k} b_i \cdot (y_i - f_i)$ for some $b_i \in K[t, y]$, $i = 0, \dots, k$. Hence, $g \in M$ and, therefore, $t^p = \mathrm{LM}(g) \in L(M)$. Since G is a standard basis, t^p is divisible by the leading monomial of some element of G which implies the result. □

SINGULAR Example 3.1.4 (integral elements).
Let $K = \mathbb{Q}$, the field of rational numbers, $I = \langle x_1^2 - x_2^3 \rangle \subset A = K[x_1, \dots, x_4]$, let $f_1 = x_3^2 - 1$ and $f_2 = x_1^2 x_2$. We want to check whether the elements $b = x_3$ (respectively x_4) are integral over $K[f_1, f_2]$ mod I.

```
ring A = 0,(x(1..4),t,y(1..2)),lp;
//For complicated examples the ordering (dp(n),dp(1),dp(k))
//is preferable.

ideal I   =x(1)^2-x(2)^3;
poly f1,f2=x(3)^2-1,x(1)^2*x(2);
poly b    =x(3);
ideal M   =t-b,y(1)-f1,y(2)-f2,I;

groebner(M);
//-> _[1]=t^2-y(1)-1          _[2]=x(3)-t
//-> _[3]=x(2)^4-y(2)         _[4]=x(1)^2-x(2)^3
```

[2] Recall that $x \gg y$ refers to a block ordering where terms in $x = (x_1, \dots, x_n)$ are always greater than terms in $y = (y_1, \dots, y_k)$.

```
b =x(4);
M =t-b,y(1)-f1,y(2)-f2,I;

groebner(M);
//-> _[1]=x(4)-t                  _[2]=x(3)^2-y(1)-1
//-> _[3]=x(2)^4-y(2)             _[4]=x(1)^2-x(2)^3
```

We see that in the first case t^2 is one of the leading monomials of the standard basis of M and, therefore, x_3 is integral over $K[\bar{f}_1, \bar{f}_2]$ with integral relation $x_3^2 - \bar{f}_1 - 1$. In the second case we see that x_4 is not integral over $K[\bar{f}_1, \bar{f}_2]$.

Proposition 3.1.5 (Criterion for finiteness). *Let K be a field, and let $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_m)$ be two sets of variables. Moreover, let $I \subset K[x]$, $J = \langle h_1, \dots, h_s \rangle \subset K[y]$ be ideals and $\varphi : K[x]/I \to K[y]/J$ a morphism, defined by $\varphi(x_i) := f_i$. Set*

$$M := \langle x_1 - f_1, \dots, x_n - f_n, h_1, \dots, h_s \rangle \subset K[x,y] ,$$

and let $>$ be a block ordering on $K[x,y]$ such that $>$ is the lexicographical ordering for y, $y_1 > \dots > y_m$, and $y \gg x$. Let $G = \{g_1, \dots, g_t\}$ be a standard basis of M with respect to this ordering.

Then φ is finite if and only if for each $j \in \{1, \dots, m\}$ there exists some $g \in G$ such that $\mathrm{LM}(g) = y_j^{\nu_j}$ for some $\nu_j > 0$.

Proof. If $g_{s_j} = y_j^{\nu_j} + \sum_{\nu=0}^{\nu_j - 1} a_{j\nu}(x, y_{j+1}, \dots, y_m) \cdot y_j^\nu \in M$ then

$$g_{s_j}\big|_{x=f} := g_{s_j}\big(f_1(y), \dots, f_n(y), y_{j+1}, \dots, y_m\big) \in J$$

for $j = 1, \dots, m$. Therefore, $y_m \bmod J$ is integral over $K[x]/I$. Using induction and the transitivity of integrality, we obtain that $y_j \bmod J$ is integral over $K[x]/I$, hence $K[y]/J$ is finite over $K[x]/I$ by Proposition 3.1.2 (2).

Conversely, the finiteness of φ guarantees, again by 3.1.2, an integral relation $y_j^{\nu_j} + \sum_{\nu=0}^{\nu_j-1} a_{j\nu}\big(f_1(y), \dots, f_n(y)\big) \cdot y_j^\nu \in J$ for suitable $a_{j\nu} \in K[x]$. Using Taylor's formula, as in the proof of Proposition 3.1.3, we obtain

$$y_j^{\nu_j} + \sum_{\nu=0}^{\nu_j - 1} a_{j\nu}(x_1, \dots, x_n) \cdot y_j^\nu \in M ,$$

and, therefore, its leading monomial, $y_j^{\nu_j}$, is an element of $L(M)$. □

SINGULAR Example 3.1.6 (finite maps).
Let $\varphi : K[a,b,c] \to K[x,y,z]/\langle xy \rangle$ be given by $a \mapsto (xy)^3 + x^2 + z$, $b \mapsto y^2 - 1$, $c \mapsto z^3$. To check whether φ is finite we have to compute a standard basis of the ideal

$$M := \langle a - (xy)^3 - x^2 - z,\ b - y^2 + 1,\ c - z^3,\ xy\rangle \subset K[a,b,c,x,y,z]$$

with respect to a block ordering $x \gg y \gg z \gg a,b,c$. We choose the lexicographical ordering $x > y > z > a > b > c$.

```
ring A  =0,(x,y,z,a,b,c),lp;
ideal M =a-(xy)^3-x2-z,b-y2+1,c-z3,xy;
ideal SM=std(M);
lead(SM);                 //get leading terms of SM
//-> -[1]=a3b      _[2]=zb      _[3]=z3
//-> _[4]=ya3      _[5]=yz      _[6]=y2
//-> _[7]=xb       _[8]=xy      _[9]=x2
kill A;
```

We see that the map is finite because z^3, y^2, x^2 appear as leading terms in the standard basis. We could also have used the built–in procedure `mapIsFinite`, which checks for finiteness (cf. below).

Remark 3.1.7. Usually the above method is not the fastest. In most cases it appears to be faster, first to eliminate the x_i from M (notations from Proposition 3.1.5) and then to compute a standard basis of $M \cap K[t,y]$ for an ordering with $t \gg y_i$, see also Exercise 3.1.3.

Remark 3.1.8. For a finite map $\varphi : A \to B$ and $M \subset A$ a maximal ideal, B/MB is a finite dimensional (A/M)–vector space. This implies that the fibres of closed points of the induced map $\phi : \operatorname{Max} B \to \operatorname{Max} A$ (cf. Appendix A) are finite sets. To be specific, let $A = K[x]/I$ and $B = K[y]/J$ (K an algebraically closed field), and let

$$\mathbb{A}^m \supset V(J) \xrightarrow{\phi} V(I) \subset \mathbb{A}^n$$

be the induced map. If $M = \langle x_1 - p_1, \dots, x_n - p_n\rangle \subset K[x]$ is the maximal ideal of the point $p = (p_1, \dots, p_n) \in V(I)$ then $MB = (J+N)/J$ with $N := \langle \varphi(x_1) - p_1, \dots, \varphi(x_n) - p_n\rangle \subset K[y]$. $V(J+N) = \phi^{-1}(p)$ is the fibre of ϕ over p, which is a finite set, since $\dim_K\big(K[y]/(J+N)\big) < \infty$.

The converse, however, is not true, not even for local rings (cf. Exercise 3.1.7). But, if $\varphi : A \to B$ is a map between local analytic K–algebras, then φ is finite if and only if $\dim_K B/\varphi(\mathfrak{m}_A)B < \infty$ (cf. Corollary 6.2.14).

We illustrate a finite and a non–finite map of varieties by a picture (cf. Figure 3.1), which is created by the following Singular session:

```
ring B  = 0,(x,y,z),dp;
ideal I = x-zy;
LIB"surf.lib";
plot(I);          // cf. Fig. 3.1
```

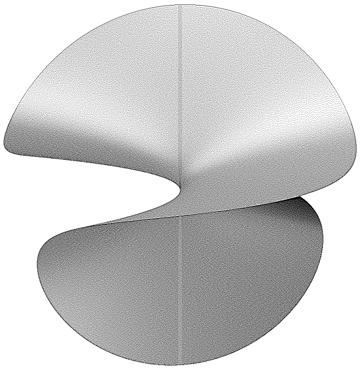

Fig. 3.1. The “blown up” (x,y)–plane.

We see that the projection ϕ_1 to the (x,y)–plane cannot be finite, since the preimage of 0 is a line. However, all fibres of the projection ϕ_2 to the (y,z)–plane consist of just one point, $\phi_2^{-1}(b,c)=(bc,b,c)$. Indeed, we can check that ϕ_2 is finite by using `mapIsFinite` from the library `algebra.lib`:

```
LIB"algebra.lib";
ring A = 0,(u,v),dp;
setring B;
map phi1 = A,x,y;      //projection to (x,y)-plane
mapIsFinite(phi1,A,I);
// -> 0
map phi2 = A,y,z;      //projection to (y,z)-plane
mapIsFinite(phi2,A,I);
// -> 1
```

Lemma 3.1.9. *Let $\varphi : A \to B$ be a ring map.*

(1) If $P \subset B$ is a prime ideal, then $\varphi^{-1}(P) \subset A$ is a prime ideal.
(2) If φ is an integral extension, and if $\varphi(x)$ is a unit in B, then $\varphi(x)$ is a unit in the ring $\varphi(A)$, too.
(3) Let φ be an integral extension, B an integral domain. Then B is a field if and only if $A/\operatorname{Ker}(\varphi)$ is a field.
(4) If φ is an integral extension and $M \subset B$ a maximal ideal, then $\varphi^{-1}(M)$ is a maximal ideal in A.

For a ring map $\varphi : A \to B$ and an ideal $I \subset B$ the ideal $\varphi^{-1}(I) \subset A$ is called the *contraction* of I; for $A \subset B$ the contraction of I is $I \cap A$.

Proof. (1) is obvious. To prove (2) let $\varphi(x)\cdot y = 1$ for some $y \in B$. Since B is integral over A, we can choose $a_0,\dots,a_{n-1} \in A$ such that

$$y^n + \varphi(a_{n-1})y^{n-1} + \cdots + \varphi(a_0) = 0\,.$$

Multiplication with $\varphi(x)^{n-1}$ gives

$$y = y^n\varphi(x)^{n-1} = -\varphi(a_{n-1} + a_{n-2}x + \cdots + a_0x^{n-1}) \in \varphi(A)\ .$$

(3) is a consequence of (2). For the if–direction, choose an integral relation as in (2) of minimal degree and use that B is integral.

Finally, (4) is a consequence of (3) because $A/\varphi^{-1}(M) \subset B/M$ is again an integral extension. □

Proposition 3.1.10 (lying over, going up). *Let $\varphi : A \to B$ be an integral extension.*

*(1) If $P \subset A$ is a prime ideal, then there is a prime ideal $Q \subset B$ such that $\varphi^{-1}(Q) = P$ (*lying over*–property) .*
*(2) Let $P \subset P' \subset A$ and $Q \subset B$ be prime ideals, with $\varphi^{-1}(Q) = P$. Then there exists a prime ideal $Q' \subset B$ such that $Q \subset Q'$ and $\varphi^{-1}(Q') = P'$ (*going up–property*).*

Proof. Let $S = A \smallsetminus P$ and consider $\varphi_P : S^{-1}A = A_P \to S^{-1}B := \varphi(S)^{-1}B$. A_P is a local ring and, therefore, for any maximal ideal $M \subset \varphi(S)^{-1}B$ we have $\varphi_P^{-1}(M) = PA_P$ (Lemma 3.1.9 (4), Exercise 3.1.2 (3)).

Now $P = \varphi_A^{-1}(M) \cap A = \varphi^{-1}(M \cap B)$ and $Q = M \cap B$ is prime (Lemma 3.1.9 (1), Exercise 3.1.2 (2)). This proves (1).

To prove (2) consider the integral extension $A/P =: \bar{A} \subset B/Q =: \bar{B}$. We apply (1) to this extension and the prime ideal $\bar{P}' \subset \bar{A}$ to obtain a prime ideal $\bar{Q}' \subset \bar{B}$ such that $\bar{Q}' \cap \bar{A} = \bar{P}'$. We set $Q' := \{q \in B \mid \bar{q} \in \bar{Q}'\}$. Then $Q' \subset B$ is a prime ideal which has the required properties. □

Remark 3.1.11. The meaning of "lying over" and "going up" is best explained geometrically. Let $\varphi^{\#} : \operatorname{Spec} B \to \operatorname{Spec} A$ denote the induced map (cf. A.3). Then lying over just means that $\varphi^{\#}$ is surjective, that is, over each point of $\operatorname{Spec} A$ lies a point of $\operatorname{Spec} B$.

Going up means that for any point $P' \in V(P)$ and any $Q \in (\varphi^{\#})^{-1}(P)$ there exists a point $Q' \in V(Q)$ such that $\varphi^{\#}(Q') = P'$, that is, the induced map $\varphi^{\#} : V(P) \to V(Q)$ is surjective, and we can "go up" from $V(Q)$ to $V(P)$.

Exercises

3.1.1. Let $A \subset B$ be rings. Show that $C := \{b \in B \mid b$ is integral over $A\}$, is a subring of B.
(Hint: consider $A[b_1, b_2]$ to show that $b_1 - b_2$, $b_1 b_2 \in C$.)

3.1.2. Check the following properties of integral dependence. Let $A \subset B \subset C$ be rings.

(1) (Transitivity) If B is integral over A and C integral over B, then C is integral over A.
(2) (Compatibility with passing to quotient rings) If $I \subset B$ is an ideal and B integral over A, then B/I is integral over $A/(I \cap A)$.

(3) (Compatibility with localization) If S is a multiplicatively closed set in A and B is integral over A, then $S^{-1}B$ is integral over $S^{-1}A$.

(4) Let $A \subset B$ be integral, $N \subset B$ a maximal ideal and $M = N \cap A$. Is B_N integral over A_M? Study the case $A = K[x^2 - 1]$, $B = K[x]$ and $N = \langle x - 1\rangle$.

3.1.3. Prove that the method for checking finiteness proposed in Remark 3.1.7 is correct. Implement both methods (that of the Proposition and of the Remark) and compare their performance.

3.1.4. (1) Let $f = x^3 - y^6$, $g = x^5 + y^3 \in K[x, y]$. Show that $K[x, y]$ is finite over $K[f, g]$ (hence, $F = (f, g) : \mathbb{A}^2 \to \mathbb{A}^2$ is a finite morphism of varieties).

(2) To find the integral relations for x and y in (1) is already difficult without a computer. Compute the first three terms of an integral relation of x over $K[f, g]$ in Example (1) by hand.

(3) Use Singular to find the integral relations for x and y in (2).

3.1.5. Let $\varphi : A \to B$ be an integral extension, and let $\psi : A \to K$ be a homomorphism to an algebraically closed field K. Prove that there exists an extension $\lambda : B \to K$ such that $\lambda \circ \varphi = \psi$.

3.1.6. Let $A \subset B_i$ be integral extensions of rings, $i = 1, \dots, s$. Prove that $A \subset \bigoplus_{i=1}^{s} B_i$ is integral.

3.1.7. Let $\varphi : A \to B$ be a ring map of Noetherian rings and $\varphi^{\#} : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ the induced map.

(1) Prove that for φ finite, $\varphi^{\#}$ has finite fibres, that is, $(\varphi^{*})^{-1}(P)$ is a finite set for each prime ideal $P \subset A$.

(2) Show that the converse of (1) is not true in general, not even if A and B are local (consider the hyperbola and $A = K[x]_{\langle x\rangle}$ where x is one variable).

3.1.8. Let K be a field and $f = y^2 + 2y - x^2 \in K[x, y]$. Prove that

(1) the canonical map $K[x] \to K[x, y]/\langle f\rangle$ is injective and finite,

(2) the induced map between local rings $K[x]_{\langle x\rangle} \to K[x, y]_{\langle x,y\rangle}/\langle f\rangle$ is injective but not finite.
(Hint: $R = K[x]_{\langle x\rangle}[y]/\langle f\rangle$ is a semi–local ring with maximal ideals $\langle x, y\rangle$ and $\langle x, y+2\rangle$. Show that $R \subset R_{y+2}$ is not finite, that is, $\frac{1}{y+2}$ is not integral over R.)

3.2 The Integral Closure

We explain the notion of integral closure by an example. Assume we have a *parametrization* of an affine plane curve which is given by a polynomial