and

$$f(P)\cdot b=1,\quad \text{that is,}\quad f(P)\neq 0 \text{ and } b=f(P)^{-1}.$$

Now suppose that $f(P)=0$ for all $P\in V(J)$; then clearly, from what I've just said, $V(J_1)=\emptyset$. So I can use (b) to deduce that $1\in J_1$, that is, there exists an expression

$$1=\sum g_i f_i + g_0(fY-1)\in k[X_1,\dots,X_n,Y] \tag{$**$}$$

with $f_i\in J$, and $g_0,g_i\in k[X_1,\dots,X_n,Y]$.

Consider the way in which Y appears in the right-hand side of $(**)$: apart from its explicit appearance in the second term, it can appear in each of the g_i; suppose that Y^N is the highest power of Y appearing in any of g_0,g_i. If I then multiply through both sides of $(**)$ by f^N, I get a relation of the form

$$f^N=\sum G_i(X_1,\dots,X_n,fY)f_i+G_0(X_1,\dots,X_n,fY)(fY-1); \tag{$***$}$$

here G_i is just $f^N g_i$ written out as a polynomial in $X_1,\dots,X_n$ and fY.

$(***)$ is just an equality of polynomials in $k[X_1,\dots,X_n,Y]$, so I can reduce it modulo $(fY-1)$ to get

$$f^N=\sum h_i(X_1,\dots,X_n)f_i\in k[X_1,\dots,X_n,Y]/(fY-1);$$

both sides of the equation are elements of $k[X_1,\dots,X_n]$. Since the natural homomorphism $k[X_1,\dots,X_n]\hookrightarrow k[X_1,\dots,X_n,Y]/(fY-1)$ is injective (it is just the inclusion of $k[X_1,\dots,X_n]$ into $k[X_1,\dots,X_n][f^{-1}]$, as a subring of its field of fractions), it follows that

$$f^N=\sum h_i(X_1,\dots,X_n)f_i\in k[X_1,\dots,X_n];$$

that is, $f^N\in J$ for some N. Q.E.D.

Remark Several of the textbooks cut the argument short by just saying that $(**)$ is an identity, so it remains true if we set $Y=f^{-1}$. This is of course perfectly valid, but I have preferred to spell it out in detail.

3.11 Worked examples

(a) Hypersurfaces. The simplest example of a variety is the hypersurface $V(f):(f=0)\subset\mathbb{A}^n_k$. If k is algebraically closed, there is just the obvious correspondence between irreducible elements $f\in k[X_1,\dots,X_n]$ and irreducible hypersurfaces: it follows from the Nullstellensatz that two distinct irreducible polynomials f_1,f_2 (not multiples of one another) define different hypersurfaces $V(f_1)$ and $V(f_2)$. This is not at all obvious (for example, it's false over $\mathbb{R}$), although it can be proved without using the Nullstellensatz by *elimination theory*, a much more explicit method with a nice 19th century flavour; see Ex. 3.13.

(b) Once past the hypersurfaces, most varieties are given by "lots" of equations; contrary to intuition, it is usually the case that the ideal $I(X)$ needs many generators, that is, many more than the codimension of X. I give an example of a curve $C\subset\mathbb{A}^3_k$ for which $I(C)$ needs 3 generators; assume that k is an infinite field.

Consider first $J = (uw - v^2, u^3 - vw)$. Then J is not prime, since

$$J \ni w(uw - v^2) - v(u^3 - vw) = u(w^2 - u^2v),$$

but $u, w^2 - u^2v \notin J$. Therefore

$$V(J) = V(J, u) \cup V(J, w^2 - u^2v);$$

obviously, $V(J,u)$ is the w-axis ($u = v = 0$). I claim that the other component $C = V(J, w^2 - u^2v)$ is an irreducible curve; indeed, C is given by

$$uw = v^2, \quad u^3 = vw, \quad w^2 = u^2v.$$

I claim that $C \subset \mathbb{A}^3$ is the image of the map $\varphi\colon \mathbb{A}^1 \to C \subset \mathbb{A}^3$ given by $t \mapsto t^3, t^4, t^5$: to see this, if $u \neq 0$ then $v, w \neq 0$. Set $t = v/u$, then $t = w/v$ and $t^2 = (v/u)(w/v) = w/u$. Hence $v = w^2/u^2 = t^4$, $u = v/(v/u) = t^4/t = t^3$, and $w = tv = t^5$. Now C is irreducible, since if $C = X_1 \cup X_2$ with $X_i \subset C$, and $f_i(u,v,w) \in I(X_i)$, then for all t, one of $f_i(t^3, t^4, t^5)$ must vanish. Since a nonzero polynomial has at most a finite number of zeros, one of f_1, f_2 must vanish identically, so $f_i \in I(C)$.

This example is of a nice 'monomial' kind; in general it might be quite tricky to guess the irreducible components of a variety, and even more so to prove that they are irreducible. A similar example is given in Ex. 3.11.

3.12 Finite algebras

I now start on the proof of (3.8). Let $A \subset B$ be rings. As usual, B is said to be *finitely generated* over A (or f.g. as A-algebra) if there exist finitely many elements $b_1, \dots, b_n$ such that $B = A[b_1, \dots, b_n]$, so that B is generated as a ring by A and $b_1, \dots, b_n$.

Contrast with the following definition: B is a *finite A-algebra* if there exist finitely many elements $b_1, \dots, b_n$ such that $B = Ab_1 + \cdots + Ab_n$, that is, B is finitely generated as A-module. The crucial distinction here is between generation as ring (when you're allowed any polynomial expressions in the b_i), and as module (the b_i can only occur linearly). For example, $k[X]$ is a finitely generated k-algebra (it's generated by one element X), but is not a finite k-algebra (since it has infinite dimension as k-vector space).

Proposition *(i) Let $A \subset B \subset C$ be rings; then*

B a finite A-algebra and C a finite B-algebra

$$\implies \quad C \text{ a finite } A\text{-algebra}.$$

(ii) If $A \subset B$ is a finite A-algebra and $x \in B$ then x satisfies a monic equation over A, that is, there exists a relation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \quad \text{with } a_i \in A$$

(note that the leading coefficient is 1).

(iii) Conversely, if x satisfies a monic equation over A, then $B = A[x]$ is a finite A-algebra.