3. Integral Extensions

Definition. Suppose R is a subring of the commutative ring S.

(1) An element $s \in S$ is integral over R if s is a root of a monic polynomial in $R[X]$.

(2) The ring S is an integral extension of R or just integral over R if every $s \in S$ is integral over R.

(3) The integral closure of R in S is the set of elements of S that are integral over R.

(4) The ring R is said to be integrally closed in S if R is equal to its integral closure in S. The integral closure of an integral domain R in its field of fractions is called the normalization of R. An integral domain is called integrally closed or normal if it is integrally closed in its field of fractions.

49. Theorem. Let R be a subring of the commutative ring S. Then the following are equivalent:

(1) s is integral over R;

(2) $R[s]$ is a finitely generated R-module;

(3) $s \in T$ for some subring T, $R \subseteq T \subseteq S$, that is a finitely generated R-module.

proof. Suppose first that (1) holds and let s be a root of the

monic polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$. Then

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

and so s^n, and then all higher powers of s, can be expressed as R-linear combinations of $s^{n-1}, \ldots, s, 1$. Hence

$$R[s] = R1 + Rs + \cdots + Rs^{n-1}$$

is finitely generated as an R-module, which gives (2).

If (2) holds, then (3) holds with $T = R[s]$.

Suppose that (3) holds and let $v_1, \ldots, v_n$ be a finite generating set for T. Then for $i = 1, \ldots, n$, $sv_i \in T$ since T is a ring, and so can be written as R-linear combination of $v_1, \ldots, v_n$:

$$sv_i = \sum_{j=1}^{n} a_{ij} v_j, \quad (a_{ij} \in R)$$

i.e.,

$$0 = \sum_{j=1}^{n} (\delta_{ij} s - a_{ij}) v_j \quad (i = 1, 2, \ldots, n)$$

where δ_{ij} is the Kronecker delta. If B is the $n \times n$ matrix whose i,j entry is $\delta_{ij} s - a_{ij}$, and v is the $n \times 1$ column vector whose entries $v_1, \ldots, v_n$, then these equations are simply

$$Bv = 0.$$

By the determinant trick, we see that $(\det B) v_i = 0$ for all i. Since $1 \in T$ is an R-linear combination of $v_1, \ldots, v_n$, it follows that $\det B = 0$. But $B = sI - A$, where $A = (a_{ij})$.

Thus s is a root of the monic polynomial $\det(xI-A) \in R[X]$, and so s is a root of a monic polynomial with coefficients in R, which gives (1), completing the proof.

50. Corollary. Let $R \subseteq S$ be an extension of commutative rings, and let $s, t \in S$.

(1) If s and t are integral over R, then so are $s \pm t$ and st.

(2) The integral closure of R in S is a subring of S containing R.

(3) Integrality is transitive: Let S be a subring of T; if T is integral over S and S is integral over R, then T is integral over R.

proof. (1) $s, t \in S$ integral over $R \Rightarrow R[s,t]$ is f.g. as an R-module.

(Remark: $R \subset R' \subset R''$: a ring tower s.t. R'' is generated over R' by $\{x_1, \dots, x_n\}$, as a module, and R' is generated over R by $\{y_1, \dots, y_m\}$, as a module.
$\Rightarrow R''$ is generated over R by $\{x_i y_j : i = 1, \dots, n,\ j = 1, \dots, m\}$ as a module.)

t integral over $R \Rightarrow t$ integral over $R[s]$.

$$\underbrace{R \subset R[s]}_{\text{f.g.}} \subset \underbrace{R[s,t]}_{\text{f.g.}} \qquad s \mp t,\ st \in R[s,t]$$

Using Theorem 49, by taking $T = R[s,t]$, we complete the proof of part (1).

We also see the part (2) from (1) using the Subring Criterion.

For the proof of part (3), let $R \subseteq S \subseteq T$ be rings, where T is int. over S and S is integral over R. Let $t \in T$. $\exists\ s_0, s_1, \ldots, s_{n-1} \in S$ s.t.

$$t^n + s_{n-1}t^{n-1} + \cdots + s_1 t + s_0 = 0 .$$

$\Rightarrow t$ is integral over $R_1 = R[s_0, s_1, \ldots s_{n-1}] \Rightarrow R_1[t]$ is a f.g. R_1-module.

$$R \subseteq R_1 \subseteq R_1[t]$$

(f.g. over R; f.g. over R_1)

By Theorem 49, we see that t is integral over R.

51. Corollary. Let $R \subset S$ be a ring extension and let $\bar{R}$ denote the integral closure of R in S. Then $\bar{R}$ is integrally closed in S.

proof. Let $\bar{\bar{R}}$ be the integral closure of $\bar{R}$ in S. Clearly $\bar{R} \subseteq \bar{\bar{R}}$. Let $s \in \bar{\bar{R}} \Rightarrow \bar{R}[s]$ int. of $\bar{R}$ & $\bar{R}$ int. over $R \Rightarrow s$ int. over R (by Corollary 50 (3)). $\Rightarrow s \in \bar{R} \Rightarrow \bar{R} = \bar{\bar{R}}$.

§2. Examples :

(i) If K/F is a field extension, then K is algebraic over F if and only if K is integral over F.

(ii) Let $R \subseteq S$ be an integral extension of rings, and let I be an ideal of S. Then one can embed $R/I\cap R$ into the factor ring S/I, in a natural way.

$$\begin{array}{ccc} R/I\cap R & \longrightarrow & S/I \\ r+(I\cap R) & \longmapsto & r+I \end{array}$$

Considering $R/I\cap R$ as a subring of S/I, we can easily conclude that S/I is integral over $R/I\cap R$.

(iii) If R is a U.F.D., then it is integrally closed: Let K denote the field of fractions of R, and let $\frac{a}{b} \in K$ $(a, b \in R,\ b \neq 0)$ be integral over R.

$$\Rightarrow \left(\frac{a}{b}\right)^n + r_1\left(\frac{a}{b}\right)^{n-1} + \cdots + r_{n-1}\frac{a}{b} + r_n = 0 \qquad (*)$$

for some $r_1, \ldots, r_n \in R$. Since R is a UFD, we may assume that a and b are coprime. Multiplying $(*)$ by b^n from both sides, we get

$$a^n + r_1 b a^{n-1} + \cdots + r_{n-1} b^{n-1} a + r_n b^n = 0,$$

or equivalently

$$a^n = -b\left(r_1 a^{n-1} + \cdots + r_{n-1} b^{n-2} a + r_n b^{n-1}\right),$$

which gives that $b \mid a^n$. It follows that every irreducible factor of b (if exists) divides a. This means that there is no irreducible element of R dividing b, or equivalently, b is unit in R. $\Rightarrow \frac{a}{b} \in R$.

(iv) By above, for any field k, the polynomial ring $k[x,y]$ is an integrally closed domain. The ideal (x^2-y^3) is prime in $k[x,y]$.

$$R = k[x,y]/(x^2-y^3) = k[\bar{x},\bar{y}] \qquad \bar{x} = x+(x^2-y^3), \quad \bar{y} = y+(x^2-y^3)$$

$$\left(\frac{\bar{x}}{\bar{y}}\right)^3 - \bar{x} = \frac{\bar{x}^3 - \bar{x}\bar{y}^3}{\bar{y}^3} = \bar{0}$$

$\bar{x}/\bar{y} \notin R$

$\therefore$ R is not integrally closed.

$R \cong k[t^2, t^3]$? (t is a variable)

53. Theorem. Let R be a commutative domain. Then

$$R = \bigcap_{P \in \operatorname{spec}(R)} R_P = \bigcap_{M \in \operatorname{Max}(R)} R_M .$$

proof. Let k be the field of fractions of R. Then $R \subseteq R_P \subseteq k$, and k is also the field of fractions of R_P for each $P \in \operatorname{spec}(R)$. It follows that

$$R \subseteq \bigcap_{P \in \operatorname{spec}(R)} R_P \subseteq \bigcap_{M \in \operatorname{Max}(R)} R_M .$$

Now let $\lambda \in \bigcap R_M$ and write $\lambda = r/s$ with $r, s \in R$, $s \neq 0$. Let $I = (Rs : r)$. Assume $I \neq R$. Then there exists a maximal ideal M of R containing I. $\frac{r}{s} = \frac{a}{t}$ for some $a \in R$, $t \in R \setminus M$. This implies that $rt = sa \in sR$, i.e., $t \in I \subseteq M$, a contradiction. Thus $1 \in I$, which gives that $\lambda = \frac{r}{s} \in R$. □

54. Lemma. Let S be a commutative ring and let $\{R_i : i \in I\}$ be a family of subrings of S. If R_i is integrally closed in S for each $i \in I$, then the subring $\bigcap_{i \in I} R_i$ is also integrally closed in S.

proof. Straightforward.

55. Lemma. Let $R \subseteq S$ be an integral extension of rings, and let U be a multiplicatively closed subset of R. Then $U^{-1}S$ is an integral extension of $U^{-1}R$.

proof. Let $\frac{s}{u} \in U^{-1}S$ with $s \in S$, $u \in U$. Since S is integral over R,

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$$

for some $n \in \mathbb{N}$, $a_0, \ldots, a_{n-1} \in R$. Dividing both sides by u^n, we get

$$\left(\frac{s}{u}\right)^n + \frac{a_{n-1}}{u}\left(\frac{s}{u}\right)^{n-1} + \cdots + \frac{a_1}{u^{n-1}}\frac{s}{u} + \frac{a_0}{u^n} = 0,$$

proving that $\frac{s}{u}$ is integral over $U^{-1}R$ since

$$\frac{a_i}{u^{n-i}} \in U^{-1}R$$

for each $i = 0, \ldots, n-1$.

□

56. Corollary Let R be a subring of the commutative ring S, and let $\bar{R}$ be the integral closure of R in S. Let U be a multiplicatively closed subset of R. Then $U^{-1}\bar{R}$ is the integral closure of $U^{-1}R$ in $U^{-1}S$.

proof. By Lemma 55, $U^{-1}\bar{R}$ is contained in the integral closure of $U^{-1}R$ in $U^{-1}S$. Let $s \in S$, $u \in U$ be such that the element $\frac{s}{u} \in U^{-1}S$ is integral over $U^{-1}R$. Then

$$\frac{s^n}{u^n} + \frac{r_{n-1}}{u_{n-1}}\frac{s^{n-1}}{u^{n-1}} + \cdots + \frac{r_1}{u_1}\frac{s}{u} + \frac{r_0}{u_0} = 0$$

for some $n \in \mathbb{N}$, $r_0, \ldots, r_{n-1} \in R$, and $u_0, \ldots, u_{n-1} \in U$. Set $v = u_0 \cdots u_{n-1}$. Multiplying the above equation through by $\frac{u^n v^n}{1}$, we can end up with some $r_0', \ldots, r_{n-1}' \in R$ such that

$$\frac{v^n s^n}{1} + \frac{r'_{n-1}}{1} \cdot \frac{v^{n-1} s^{n-1}}{1} + \cdots + \frac{r'_1}{1} \frac{vs}{1} + \frac{r'_0}{1} = 0.$$

Hence there exists $v' \in U$ s.t.

$$v'(v^n s^n + r'_{n-1} v^{n-1} s^{n-1} + \cdots + r'_1 vs + r'_0) = 0,$$

so that $v'vs \in \bar{R}$, and $\frac{s}{u} = \frac{v'vs}{v'vu} \in U^{-1}\bar{R}$. This completes the proof. □

57. Corollary. Let R be an integral domain. The the following statements are equivalent:

(1) R is integrally closed.
(2) R_P is integrally closed for every $P \in \operatorname{spec}(R)$.
(3) R_M is integrally closed for every $M \in \operatorname{Max}(R)$.

proof. (1) $\Rightarrow$ (2): Clear by Corollary 56.
(2) $\Rightarrow$ (3): Immediate.
(3) $\Rightarrow$ (1): Follows by Theorem 53 and Lemma 54. □

58. Proposition. Suppose R is an integrally closed domain with field of fractions k, and α is an element of an extension field K of k. Then α is integral over R if and only if α is algebraic over k and the minimal polynomial of α over k lies in $R[X]$.

proof. Since the "if" part is obvious, we shall prove only the other part. Assume that $\alpha \in K$ is integral over

R. There exists a monic polynomial $P(X) \in R[X]$ s.t. $P(\alpha)=0$. Since $P(X)$ lies also in $k[X]$, α is algebraic over k. Let $m(X)$ be the minimal polynomial of α over k. Then $m(X) \mid p(X)$. Let $\alpha_1=\alpha, \ldots, \alpha_n$ be all roots of $m(X)$ (in an algebraic closure of k). Since $m(\alpha_i)=0$ for each $i=1,\ldots,n$ and $m(x) \mid p(x)$, $P(\alpha_i)=0$ for each $i=1,\ldots,n$. Then each α_i is integral over R. Define $s_j = \sum_{1 \le i_1 < \ldots < i_j \le n} (-1)^j \alpha_{i_1} \ldots \alpha_{i_j}$ for every $j=1,\ldots,n$. Since

$$m(X) = X^n + s_1 X^{n-1} + \cdots + s_n \in k[X],$$

each s_j lies in k. Also, by its definition, each s_j is integral over R. Since R is int. clsd., $s_j \in R$ $\forall j$, and so $m(X) \in R[X]$, completing the proof. □

59. Corollary. Suppose R is an integrally closed domain with field of fractions k, and $P(X) \in R[X]$ is a monic polynomial. If $P(X) = a(X)\,b(X)$ with monic polynomials $a(X), b(X) \in k[X]$, then $a(X), b(X) \in R[X]$.

Proof. We use induction on $n = \deg a(X)$. If $n=1$, then $a(X)=X-c$ for some $c \in k$. But then $P(c)=0$, and so c is integral over R. Thus $c \in R$, so that $a(X) \in R[X]$. Now let $n>1$ and assume that the corollary is true for a product in which one factor has degree less than n. Extend k to K so that K includes a root α of $a(X)$. Since α is also a root of $P(X)$, it is integral over

R, and hence it is algebraic over k with the minimal polynomial, say $m(x)$, lying in $R[X]$. $m(x) \mid a(x)$. Let $a(x) = m(x)\, a_1(x)$. If $a(x) = m(x)$, then we are done. Otherwise, $1 \leq \deg a_1(x) < \deg a(x)$, and by induction hypothesis $a_1(x) \in R[X]$ since $p(x) = a_1(x)(m(x)b(x))$. So $a(x) \in R[X]$. By symmetry, we also see that $b(x) \in R[X]$. □

60. Corollary. Let $R \subseteq S$ be an integral extension of rings where S is a domain and R is integrally closed. Let P be a prime ideal of R, and let $s \in PS$. Then with the exception of the leading term the coefficients of the minimal polynomial of s over k are elements of P.

proof. We can write $s = p_1 s_1 + \cdots + p_m s_m$ for some $p_1, \ldots, p_m \in P$ and $s_1, \ldots, s_m \in S$. Since $s_1, \ldots, s_m$ are all integral over R, the subring $T = R[s_1, \ldots, s_m]$ is a finitely generated R-module. Now $s \in PT$. Using the determinant argument (as in the proof of Theorem 49), we can find a monic polynomial

$$P(X) = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

s.t. $a_0, \ldots, a_{n-1} \in P$ and $P(s) = 0$. Let $m(x)$ be the minimal polynomial of s over k. $m(x) \mid P(x)$. Write $p(x) = m(x)\, b(x)$ for some $b(x) \in k[X]$. By Corollary 59, $m(x), b(x) \in R[X]$. If we write $\overline{a(x)}$ for any $a(x) \in R[X]$ to denote the image of $a(x)$ in $(R/p)[X]$ under

the natural hom. $R[X] \to (R/P)[X]$, we obtain

$$X^n = \overline{m(x)} \cdot \overline{b(x)},$$

which gives that $\overline{m(x)}$ and $\overline{b(x)}$ are powers of X, completing the proof. □

61. Lemma Let $f: R \to S$ be a homomorphism of commutative rings, and let $P \in \operatorname{spec}(R)$. Let extension and contraction notation for ideals be used in conjunction with f. Then P is the contraction of a prime ideal in S if and only if $P^{ec} = P$.

proof. Exercise!

10. Exercise Prove Lemma 61. [Hint: localize S at $f(R \setminus P)$].

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \chi \downarrow & & \downarrow \chi \\ R_P & \xrightarrow[\bar{f}]{} & u\text{'s} \end{array} \qquad u = f(R \setminus P)$$

$f: R \to S$ $\quad M \in \mathrm{Max}(S) \Rightarrow f^{-1}(M)$ need not be in $\mathrm{Max}(R)$.

$P \in \mathrm{spec}(R) \Rightarrow PS$ need not be in $\mathrm{Spec}(S)$

$(\mathbb{Z} \to \mathbb{Q} \quad P = 2\mathbb{Z} \quad P\mathbb{Q} = \mathbb{Q}.)$

P need not be a contraction of a prime ideal in S.

62. Theorem. Let R be a subring of the commutative ring S and suppose that S is integral over R.

(1) Assume that S is an integral domain. Then R is a field if and only if S is a field.

(2) (The Lying-over theorem) Let $P \in \mathrm{spec}(R)$. Then there exists a prime ideal Q of S s.t. $P = Q \cap R$. (In this case we say that Q is lying over P.) Moreover, P is maximal iff Q is maximal.

(3) (The Going-up Theorem) Let $P_1 \subseteq P_2 \subseteq \ldots \subseteq P_n$ be a chain of prime ideal of R and suppose that there are prime ideals $Q_1 \subseteq Q_2 \subseteq \ldots \subseteq Q_m$ of S with $P_i = Q_i \cap R$, $1 \le i \le m$ and $m < n$. Then the ascending chain of prime ideals can be completed: there are prime ideals $Q_{m+1} \subseteq \ldots \subseteq Q_n$ of S with $P_i = Q_i \cap R$ for all i.

(4) (The Going-down Theorem) Assume that S is an integral domain and R is integrally closed. Let $P_1 \supseteq P_2 \supseteq \dots \supseteq P_n$ be a chain of prime ideals of R and suppose that there are prime ideal $Q_1 \supseteq Q_2 \supseteq \dots \supseteq Q_m$ of S with $P_i = Q_i \cap R$, $1 \le i \le m$ and $m < n$. Then the descending chain of ideals can be completed: there are prime ideals $Q_{m+1} \supseteq \dots \supseteq Q_n$ of S s.t. $Q_i \cap R = P_i$ for all i.

proof. (1) Let R be a field and let $s \in S \setminus \{0\}$.

$$s^n + a_{n-1}s^{n-1} + \dots + a_1 s + a_0 = 0$$

for some $a_0, \dots, a_{n-1} \in R$. We may choose n to be the smallest with this property. Then $a_0 \neq 0$. Since

$$s(s^{n-1} + a_{n-1}s^{n-2} + \dots + a_1) = -a_0,$$

s is unit in S. Conversely assume that S is a field and let $r \in R \setminus \{0\}$. Then

$$r^{-n} + a_{n-1}r^{-n+1} + \dots + a_1 r^{-1} + a_0 = 0$$

for some $a_0, \dots, a_{n-1} \in R$. Multiplying both sides by r^{n-1}, we get

$$r^{-1} = -(a_{n-1} + \dots + a_1 r^{n-2} + a_0 r^{n-1}) \in R.$$

(2) We first prove the second statement of part (2). To this end let $P \in \operatorname{spec}(R)$ and $Q \in \operatorname{spec}(S)$ with $P = Q \cap R$.

We can embed R/p into S/Q. By Example 52 (ii), S/Q is an integral ext. of R/p, in which case S/Q is a field iff R/p is a field, or equivalently, Q is max. iff P is max.

For the remaining part, let $U = R \setminus P$. So U is a m.c. subset of both R and S. Then the following diagram commutes:

$$\begin{array}{ccc} R & \longrightarrow & U^{-1}R = R_p \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle i} \\ S & \longrightarrow & U^{-1}S \end{array}$$

where the vertical maps are inclusions. By Lemma 55, $U^{-1}S$ is integral over R_p. Let M be any maximal ideal of $U^{-1}S$. Then by what we have just shown above, $M \cap R_p = PR_p$. Now the contraction of $M \cap R_p$ to R is just P. Put another way, the preimage of M by the maps along the top and right of the diagram above is P. (i.e. $M \cap R = P$) If $Q \subseteq S$ denotes the preimage of M along the bottom of the diagram, then Q is a prime ideal of S whose contraction to R must be P because of the commutativity of the diagram.

(3) It suffices to prove that if $P_1 \subseteq P_2$ and Q_1 is a prime ideal of S with $Q_1 \cap R = P_1$, then there exists a prime Q_2 of S with $Q_1 \subseteq Q_2$ and $Q_2 \cap R = P_2$. Since

$\bar{S} = S/Q_1$ is an integral extension of $\bar{R} = R/P_1$, the first part of (2) shows that there exists a prime $\bar{Q}_2$ of $\bar{S}$ with $\bar{Q}_2 \cap \bar{R} = P_2/P_1$. Then the preimage Q_2 of $\bar{Q}_2$ in S is a prime ideal containing Q_1 with $Q_2 \cap R = P_2$.

(4) By induction, it is enough to show that given a pair of prime ideals $P_2 \subseteq P_1$ of R and a prime ideal Q_1 of S with $Q_1 \cap R = P_1$, there exists a prime ideal Q_2 of S contained in Q_1 with $Q_2 \cap R = P_2$. It is clear $P_2 \subseteq P_2 S_{Q_1} \cap R$. Let k denote the field of fractions of R. Choose $s \in P_2 S$ and $d \in S \setminus Q_1$ such that $a = s/d$ lies in R. (Note that $P_2 S_{Q_1}$ is just the extension of the ideal $P_2 S$ in S w.r.t. the natural hom. $S \to S_{Q_1}$.) Let $m(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ be the minimal polynomial of s over k. By Corollary 60, $a_0, a_1, \ldots, a_{n-1} \in P_2$. Let $b(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0$ with $b_i = \frac{a_i}{a^{n-i}}$. Then clearly d is a root of $b(X)$. Since we also have $a^n b(X) = m(aX)$, $b(X)$ is irreducible in $k[X]$, showing that $b(X)$ is the minimal polynomial of d over k. By Proposition 58, we must have $b_i \in R$ for every $i = 0, 1, \ldots, n-1$. If $b_i \in P_2$ for every i, then since $b(d) = 0$, $d^n \in P_2 S \subseteq P_1 S \subseteq Q_1$, a contradiction. Thus $b_i \notin P_2$ for some i, and hence $a \in P_2$ (since $a^{n-i} b_i = a_i \in P_2$). It follows that $P_2 S_{Q_1} \cap R = P_2$. If we use

Lemma 61 for the inclusion map $R \to S_{Q_1}$, we can find a prime ideal P in S_{Q_1} with $P \cap R = P_2$. Let $Q_2 = P \cap S$. Since P is a proper ideal of S_{Q_1}, we have $P \subseteq Q_1 S_{Q_1}$, so that $Q_2 = P \cap S \subseteq Q_1 S_{Q_1} \cap S = Q_1$. On the other hand, $Q_2 \cap R = P \cap S \cap R = P \cap R = P_2$. This completes the proof. □

63. Corollary. Suppose R is a subring of the ring S and assume that S is integral and finitely generated (as a ring) over R. If P is a maximal ideal in R, then there are finitely many maximal ideals Q of S with $Q \cap R = P$.

proof. Let $S = R[s_1, \ldots, s_n]$. Let Q be a maximal ideal of S with $Q \cap R = P$. Note that

$$S/Q = (R/P)[\bar{s}_1, \ldots, \bar{s}_n],$$

where $\bar{s}_i$ denotes the element $s_i + Q$ in S/Q, and that Q is the kernel of the homomorphism

$$S = R[s_1, \ldots, s_n] \xrightarrow{\varphi} (R/P)[\bar{s}_1, \ldots, \bar{s}_n] = S/Q$$

defined by $r \mapsto r + P$ for $r \in R$ and $s_i \mapsto \bar{s}_i$. Let s_i be a root of a monic polynomial $p_i(x) \in R[x]$ for $i = 1, \ldots, n$. Then $\bar{s}_i$ is a root of the monic polynomial $\bar{p}_i(x) \in (R/P)[x]$, where $\bar{p}_i(x)$ is obtained by reducing the coefficients of $p_i(x)$ module P. Since there are only a finite number of possible roots of $p_i(x)$ (in a fixed algebraic closure of R/P), there

are finitely many homomorphisms φ from S into a field extension of R/p (in a fixed algebraic closure of R/p) that extend the natural homomorphism from R onto R/p. Since maximal ideals of S are in one-to-one correspondence with such homomorphisms φ, the proof is complete. □

Definition. Let K be an extension field of $\mathbb{Q}$.
(1) An element $\alpha \in K$ is called an algebraic integer if α is integral over $\mathbb{Z}$.
(2) The integral closure of $\mathbb{Z}$ in K is called the ring of integers of K, and is denoted by $\mathcal{O}_K$.

An algebraic integer is clearly algebraic over $\mathbb{Q}$, so the ring of all algebraic integers is the ring of integers in $\overline{\mathbb{Q}}$, an algebraic closure of $\mathbb{Q}$. Note that the algebraic integers in $\mathbb{Q}$ are the integers $\mathbb{Z}$, i.e., $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, because $\mathbb{Z}$ is an algebraically closed domain (as it is a UFD).

By Proposition 58, we see that an element α in some field extension of $\mathbb{Q}$ is an algebraic integer if and only if α is algebraic over $\mathbb{Q}$ and its minimal polynomial has integer coefficients.

The elements of $\mathbb{Z}$ are sometimes referred to as "rational integer" to distinguish them from the "integers" in extensions of finite degree over $\mathbb{Q}$ (called number fields).

Let E/k be a finite extension of fields. Then there are only a finite number distinct homomorphisms over k from E into an algebraic closure $\bar{E}$ of E. Let $\sigma_1, \ldots, \sigma_n$ be all distinct embeddings of E in $\bar{E}$. It follows that the extension

$$K = (\sigma_1 E) \ldots (\sigma_n E),$$

which is the compositum of all these embeddings, is a finite normal extension of k because for any embedding of K, say τ, we can apply τ to each extension $\sigma_i E$. Then $(\tau\sigma_1, \ldots, \tau\sigma_n)$ is a permutation of $(\sigma_1, \ldots, \sigma_n)$ and thus τ maps K into itself. Hence K is the smallest normal extension of k containing E, called a normal closure of E over k.

For the finite extension E/k of fields (with the additional assumption $\mathrm{char}(k)=0$), we define the trace

$$\mathrm{Tr}_{E/k}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha),$$

where $\alpha \in E$. Notice that if K is as above, then

$Gal(K/k) = \{\sigma_1, \ldots, \sigma_n\}$. Since K/k is a Galois extension and $Tr_{E/k}(\alpha)$ is left fixed under all the $\sigma_1, \ldots, \sigma_n$, $Tr_{E/k}(\alpha) \in k$. Note that $Tr_{E/k}$ is a k-linear map from E into k. It should be also noted that if

$$p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in k[x]$$

is the minimal polynomial of α over k, then $Tr_{E/k}(\alpha) = -a_{d-1}$.

For any integral domain R, the rank of an R-module M is the maximum number of R-linearly independent elements of M. If K is the field of fractions of R and M is a torsion-free R-module of rank m, then $M \otimes_R K$ is an m-dimensional vector space over K; in fact if any of rank M or $\dim_K(M \otimes_R K)$ is finite, then rank $M = \dim_K(M \otimes_R K)$. This gives, in particular, that if M and N are two torsion-free R-modules of finite ranks m and n, respectively, with $M \subseteq N$, then $m \leq n$.

64. Theorem Let K be a number field of degree n over $\mathbb{Q}$.

(1) The ring $\mathcal{O}_K$ of integers in K is a Noetherian ring and is a free $\mathbb{Z}$-module of rank n.

(2) For every $\beta \in K$, there is some nonzero $d \in \mathbb{Z}$ such that $d\beta$ is an algebraic integer. In particular, K is the field of fractions of $\mathcal{O}_K$.

(3) If $\beta_1, \ldots, \beta_n$ is any $\mathbb{Q}$-basis of K, then there exists an integer

d such that $d\beta_1, \ldots, d\beta_n$ is a basis for a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank n. Any basis of the $\mathbb{Z}$-module $\mathcal{O}_K$ is also a basis for K as a vector space over $\mathbb{Q}$.

proof. Let $\beta \in K$, and let $x^k + a_{k-1}x^{k-1} + \cdots + a_0$ be the minimal polynomial of β over K. If d is a common denominator for the coefficients, then multiplying through by d^k shows that

$$(d\beta)^k + da_{k-1}(d\beta)^{k-1} + \cdots + d^{k-1}a_1(d\beta) + d^k a_0 = 0,$$

and $d^k a_0, d^{k-1}a_1, \ldots, da_{k-1} \in \mathbb{Z}$. Hence $d\beta \in \mathcal{O}_K$, which proves the first part of (2), and then the second statement in (2) follows immediately.

If $\beta_1, \ldots, \beta_n$ are a $\mathbb{Q}$-basis for K over $\mathbb{Q}$, then there is a nonzero integer d such that $d\beta_1, \ldots, d\beta_n$ all lie in $\mathcal{O}_K$. These elements are still linearly independent over $\mathbb{Q}$, so in particular are independent over $\mathbb{Z}$, hence generate a free submodule of $\mathcal{O}_K$ of rank n, which proves the first statement in (3).

Since $\mathcal{O}_K$ is a subring of the field K, it is a torsion-free $\mathbb{Z}$-module. If $\mathcal{O}_K$ were contained in some finitely generated $\mathbb{Z}$-module it would follow that $\mathcal{O}_K$ is also finitely generated over $\mathbb{Z}$, hence is a free $\mathbb{Z}$-module. If L is a normal closure of K (in some algebraic closure of $\mathbb{Q}$), then $\mathcal{O}_K \subseteq \mathcal{O}_L$ and so it suffices to see that $\mathcal{O}_L$ is contained in a finitely generated $\mathbb{Z}$-module. Note that L is a finite extension of K, and so it is a finite extension of $\mathbb{Q}$, by transitivity of dimensionality. Let $\alpha_1, \ldots, \alpha_m$ be a $\mathbb{Q}$-basis for

L over $\mathbb{Q}$. Multiplying by an integer d, if necessary, we may assume that each α_i is an algebraic integer, i.e., $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_L$. For each fixed $\theta \neq 0$ in L, the map

$$T_\theta : L \longrightarrow \mathbb{Q} \quad \text{defined by} \quad T_\theta(\alpha) = \mathrm{Tr}_{L/\mathbb{Q}}(\theta\alpha)$$

is a $\mathbb{Q}$-linear transformation. $T_\theta \neq 0$ because $T_\theta(\theta^{-1}) = \mathrm{Tr}_{L/\mathbb{Q}}(1) = m$. It follows that the map

$$\begin{aligned} L &\longrightarrow \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{Q}) \\ \theta &\longmapsto T_\theta \end{aligned}$$

is an injective homomorphism of vector spaces over $\mathbb{Q}$. Since both spaces have the same dimension over $\mathbb{Q}$, the map is an isomorphism; in other words, every linear functional on L is of the form T_θ for some $\theta \in L$. In particular, there are elements $\alpha_1', \ldots, \alpha_m'$ in L such that $\{T_{\alpha_1'}, \ldots, T_{\alpha_m'}\}$ give the dual basis of $\alpha_1, \ldots, \alpha_m$, i.e.

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i'\alpha_j) = \begin{cases} 1, & \text{if } i=j \\ 0, & \text{otherwise.} \end{cases}$$

Since $\alpha_1', \ldots, \alpha_m'$ are linearly independent, they give a basis for L over $\mathbb{Q}$. Hence every element $\beta \in \mathcal{O}_L$ can be written

$$\beta = a_1\alpha_1' + \cdots + a_i\alpha_i' + \cdots + a_m\alpha_m'$$

with $a_1, \ldots, a_m \in \mathbb{Q}$. Multiplying by α_j and taking the trace shows that

$$\begin{aligned} \mathrm{Tr}_{L/\mathbb{Q}}(\beta\alpha_j) &= a_1\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_1'\alpha_j) + \cdots + a_i\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i'\alpha_j) + \cdots + a_m\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_m'\alpha_j) \\ &= a_j. \end{aligned}$$

But β and α_j are both elements of $\mathcal{O}_L$, so also $\beta\alpha_j \in \mathcal{O}_L$,

and this implies that $a_j = Tr_{L/\mathbb{Q}}(\beta\alpha_j) \in \mathbb{Z}$ since we know that the trace of $\beta\alpha_j$ is a coefficient of the minimal polynomial of $\beta\alpha_j$ over $\mathbb{Q}$, which is an element of $\mathbb{Z}[X]$, as noted above. It follows that

$$\mathcal{O}_L \subseteq \mathbb{Z}\alpha_1' + \cdots + \mathbb{Z}\alpha_m'$$

so that $\mathcal{O}_L$ is contained in a finitely generated $\mathbb{Z}$-module, proving that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module.

Since we can embedd $\mathcal{O}_K \otimes \mathbb{Q}$ into K in a natural way, we have $\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K = \dim_{\mathbb{Q}}(\mathcal{O}_K \otimes \mathbb{Q}) \leq \dim_{\mathbb{Q}} K = n$. Because $\mathcal{O}_K$ also contains a free $\mathbb{Z}$-module of rank n, it follows that the $\mathbb{Z}$-rank of $\mathcal{O}_K$ is precisely n. Note that any $\mathbb{Z}$-linear dependence relation among elements in $\mathcal{O}_K$ is a $\mathbb{Q}$-linear dependence relation in K, and multiplying a $\mathbb{Q}$-linear dependence relation of elements of $\mathcal{O}_K$ in K by a common denominator for the coefficients yields a $\mathbb{Z}$-linear dependence relation in $\mathcal{O}_K$. Thus the second statement in (3) follows.

Finally, any ideal I in $\mathcal{O}_K$ is a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module of rank n, so is a free $\mathbb{Z}$-module of rank at most n, and a set of $\mathbb{Z}$-module generators for I is also a set of $\mathcal{O}_K$-generators. Hence every ideal of $\mathcal{O}_K$ can be generated by at most n elements, which implies that $\mathcal{O}_K$ is a Noetherian ring and completes the proof.

□

Definition. An *integral basis* for the number field K is a basis of the ring of integers in K considered as a free $\mathbb{Z}$-module of

rank $[K:\mathbb{Q}]$.

If P is a nonzero prime ideal in the ring of integers $\mathcal{O}_K$ of a number field K, then $P\cap\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. If $0\neq\alpha\in P$, then the constant term of the minimal polynomial for α over $\mathbb{Q}$ is then an element in $P\cap\mathbb{Z}$, which shows that $P\cap\mathbb{Z}\neq 0$; hence $P\cap\mathbb{Z}=p\mathbb{Z}$ for some prime number p. By Theorem 62, every prime ideal (p) in $\mathbb{Z}$ arises in this way. Since $p\mathbb{Z}$ is maximal, it follows, from (2) in Theorem 62, that nonzero prime ideals P in $\mathcal{O}_K$ are maximal, and then by Corollary 63, there are finitely many prime ideals P in $\mathcal{O}_K$ with $P\cap\mathbb{Z}=p\mathbb{Z}$.

65. Example. (The ring of integers in quadratic extensions of $\mathbb{Q}$)

Let K be a field extension of $\mathbb{Q}$ with $[K:\mathbb{Q}]=2$. Then there exists $\alpha\in K$ such that $K=\mathbb{Q}(\alpha)$. The minimal polynomial of α has degree 2, so that $\alpha^2+a\alpha+b=0$ for some $a,b\in\mathbb{Q}$. Let $\beta=\alpha+\frac{a}{2}$. Then $0=(\beta-\frac{a}{2})^2+a(\beta-\frac{a}{2})+b=\beta^2-a\beta+\frac{a^2}{4}+a\beta-\frac{a^2}{2}+b$, which implies $\beta^2=\frac{a^2}{4}-b\in\mathbb{Q}$ but $\beta\notin\mathbb{Q}$ since $\alpha\notin\mathbb{Q}$. It follows that $K=\mathbb{Q}(\beta)$ and $\beta^2\in\mathbb{Q}$. There is an integer $e\in\mathbb{Z}$ such that $e^2\beta^2=d\in\mathbb{Z}$. Now $K=\mathbb{Q}(\sqrt{d})$. Notice that we may choose a square-free integer D such that $K=\mathbb{Q}(\sqrt{D})$. Then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})}=\mathbb{Z}[\omega]=\mathbb{Z}\cdot 1+\mathbb{Z}\cdot\omega,$$

with integral basis $1,\omega$, where

$$\omega = \begin{cases} \sqrt{D}, & \text{if } D \equiv 2,3 \pmod 4 \\ \dfrac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

This is called the quadratic integer ring.

proof. Since ω satisfies $\omega^2 - D = 0$ (respectively, $\omega^2 - \omega + \frac{1-D}{4} = 0$) for $D \equiv 2,3 \pmod 4$ (respectively, $D \equiv 1 \pmod 4$), it follows that ω is an algebraic integer in K and so $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$. To prove that this is the full ring of integers in K, let $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$, and suppose that α is an algebraic integer. If $b = 0$, then $\alpha \in \mathbb{Q}$, and so $a \in \mathbb{Z}$. If $b \neq 0$, the minimal polynomial of α is

$$X^2 - 2aX + (a^2 - b^2 D).$$

Then Proposition 56 shows that $2a$ and $a^2 - b^2 D$ are integers. Then $4(a^2 - b^2 D) = (2a)^2 - (2b)^2 D \in \mathbb{Z}$, hence $(2b)^2 D \in \mathbb{Z}$. Since D is square-free, it follows that $2b \in \mathbb{Z}$. Write $a = x/2$ and $b = y/2$ for some integers x and y. Since $a^2 - b^2 D \in \mathbb{Z}$, $x^2 - y^2 D \equiv 0 \pmod 4$. Since 0 and 1 are the only squares modulo 4 and D is not divisible by 4, it is easy to check that the only possibilities are the following:

(i) $D \equiv 2$ or $3 \pmod 4$ and x, y are both even, or

(ii) $D \equiv 1 \pmod 4$ and x, y are both even or both odd.

In case (i), $a, b \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}[\omega]$. In case (ii), $a + b\sqrt{D} = r + s\omega$ where $r = (x-y)/2$ and $s = y$ are both integers, so again $\alpha \in \mathbb{Z}[\omega]$.

Definition. If k is a field the elements $y_1, \ldots, y_q$ in some k-algebra are called algebraically independent over k if there is no nonzero polynomial p in q variables over k such that $p(y_1, \ldots, y_q) = 0$.

Thus $y_1, \ldots, y_q$ are algebraically independent if and only if the k-algebra homomorphism from the polynomial ring $k[X_1, \ldots, X_q]$ to $k[y_1, \ldots, y_q]$ defined by $X_i \mapsto y_i$ is an isomorphism. Elements in a field extension of k are algebraically independent over k if and only if they are independent transcendentals over k.

66. Theorem (Noether's Normalization Theorem) Let k be a field and suppose that $A = k[r_1, \ldots, r_m]$ is a finitely generated k-algebra. Then either A is an algebraic field extension of k or for some q, $1 \leq q \leq m$, there are algebraically independent elements $y_1, \ldots, y_q \in A$ such that A is integral over $k[y_1, \ldots, y_q]$.

proof. Proceed by induction on m. Let $m = 1$. Then $A = k[r_1]$. If r_1 is transcendental, then take $y_1 = r_1$; otherwise, A is an algebraic field extension of k. Now let $m > 1$ and suppose that the theorem is true for positive integers smaller than m. If $r_1, \ldots, r_m$ are algebraically independent over k, then $y_i = r_i$ $(1 \leq i \leq m)$, and the proof is complete. Otherwise, there exists $0 \neq f(X_1, \ldots, X_m) \in k[X_1, \ldots, X_m]$ such that $f(r_1, \ldots, r_m) = 0$. The polynomial f is a sum of monomials of the form $aX_1^{e_1} \ldots X_m^{e_m}$, where the degree of this monomial is $e_1 + \cdots + e_m$ and the degree, say d, of f is the maximum of

the degrees of its monomials. Renumbering the variables, if necessary, we may assume that f is a nonconstant polynomial in X_m with coefficients in the ring $k[X_1, \ldots, X_{m-1}]$.

Define the integers $a_i = (1+d)^i$ and new variables

$$Y_i = X_i - X_m^{a_i} \quad \text{for } 1 \le i \le m-1.$$

Let $g(Y_1, \ldots, Y_{m-1}, X_m) = f(Y_1 + X_m^{a_1}, \ldots, Y_{m-1} + X_m^{a_{m-1}}, X_m)$, so $g \in k[Y_1, \ldots, Y_{m-1}, X_m]$. Each monomial term of f contributes a single term of the form a constant times X_m^e to g. It is also easy to check that the choice of a_i ensures that distinct monomials of f give different values of e (for example by viewing the degrees of the monomials in the new variables as integers expressed in base $d+1$). If N is the highest power of X_m that occurs, then it follows that

$$g = cX_m^N + \sum_{i=0}^{N-1} h_i(Y_1, \ldots, Y_{m-1}) X_m^i$$

for some nonzero $c \in k$. If now $s_i = r_i - r_m^{a_i}$, then

$$\frac{1}{c} g(s_1, \ldots, s_{m-1}, r_m) = \frac{1}{c} f(r_1, \ldots, r_{m-1}, r_m) = 0,$$

which shows that r_m is integral over $B = k[s_1, \ldots, s_{m-1}]$. Each r_i for $1 \le i \le m-1$ lies in $B[r_m]$, which shows that $A = B[r_m]$. It follows that A is integral over B. Since B is a k-algebra generated by $m-1$ elements, induction completes the proof.

□

A polynomial $f \in k[X_1, \ldots, X_n]$ with coefficients in a field k defines a function, $f : k^n \to k$; the value of f at a point $(a_1, \ldots, a_n) \in k^n$ is obtained by substituting the a_i for the X_i in f. The function defined by f is called a <u>polynomial function</u> on the n-dimensional vector space k^n over k, with values in k. If k is infinite, then no polynomial function other than 0 can vanish identically on k^n. To see this consider a polynomial $f(X_1, \ldots, X_n)$ in n variables. If $n = 1$, the above statement follows from the fact that a polynomial in one variable can have only finitely many roots. If $n > 1$, considering $f(X_1, \ldots, X_n)$ as a polynomial in $n-1$ variables with coefficients that are polynomials in one variable, by the case $n = 1$, we can specialize this one to a scalar in such a way that the polynomial remains nonzero, and we are done by induction on the number of variables. It follows that if k is infinite, distinct polynomials define distinct functions. Thus we may regard the polynomial ring $k[X_1, \ldots, X_n]$ as the ring of polynomial functions on k^n. Viewed with its ring of polynomial functions, k^n is usually referred to as <u>affine n-space</u> over k, written $\mathbb{A}^n(k)$ or simply $\mathbb{A}^n$.

Given a subset $I \subseteq k[X_1, \ldots, X_n]$, we define a corresponding <u>algebraic subset</u> of k^n to be

$$Z(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}.$$

Such algebraic sets are sometimes called <u>affine algebraic sets</u>.

It is easy to see that

$$Z(I) = Z(Ik[x_1,\ldots,x_n])$$

for any subset $I \subseteq k[x_1,\ldots,x_n]$.

If $X = Z(I)$ is an algebraic set, then an <u>algebraic subset</u> $Y \subseteq X$ is a set of the form $Y = Z(J)$ that happens to be contained in X. A non-empty algebraic set is called <u>irreducible</u> if it is not the union of two non-empty smaller algebraic subsets. Irreducible algebraic sets are called <u>algebraic varieties</u>.

If $k = \mathbb{R}$ or $\mathbb{C}$, then k^r is naturally a topological space (as a product of copies of k), and an algebraic subset $X \subseteq \mathbb{A}^r$ inherits the subspace topology, called the <u>classical topology</u>. But there is another, coarser, topology on X that is defined over any field. Polynomial functions on X will play the role of continuous functions, even when the fields we are working over have no topology, and by analogy with the continuos case it is natural to think of an algebraic subset Y as a closed subset of X. Since we obviously have

$$\cap_i Z(J_i) = Z(\cup_i J_i),$$

the intersection of any collection of algebraic subsets is algebraic. Furthermore, if we define $\prod_{i=1}^{n} J_i$ to be the set consisting of all products of one function from each J_i, then $\bigcup_{i=1}^{n} Z(J_i) = Z(\prod_{i=1}^{n} J_i)$, so any finite union of algebraic subsets is algebraic. Thus we may define a topology on X by taking the closed sets to be the algebraic

subsets of X. This topology is called the Zariski topology. The Zariski topology is much coarser than the classical topology when $k=\mathbb{R}$ or $\mathbb{C}$, but it is still quite useful.

Given any subset $X \subseteq k^n$, we define

$$\mathcal{I}(X) = \{ f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in X \}.$$

It is clear that $\mathcal{I}(X)$ is an ideal. A polynomial function on X is by definition the restriction of a polynomial function on k^n to X. Identifying two polynomial functions if they agree at all the points of X, we get the coordinate ring $A(X)$ of X. Clearly, we have $A(X) = k[x_1, \ldots, x_n]/\mathcal{I}(X)$.

Not every homomorphic image $A = k[x_1, \ldots, x_n]/I$ could be the coordinate ring of a set. For suppose an element $f \in A$ satisfies $f^d = 0$. If f were a function on some set X, then $0 = f^d(p) = f(p)^d$, which gives that $f(p) = 0$ for all $p \in X$ since the values of f are elements of k, a field. Thus f itself is the zero element of $A(X)$. In general, a ring is said to be reduced if its only nilpotent element is 0; we have just shown that $A(X)$ is reduced.

We call an ideal I of any commutative ring R a radical ideal if $I = \sqrt{I}$. Clearly, for an ideal I of R, I is a radical ideal if and only if R/I is reduced. Above remarks show that the ideals $\mathcal{I}(X)$ are radical ideals. However, not every radical ideal arises as $\mathcal{I}(X)$ for some subset $X \subseteq A$: For example, the

ideal $I = (X^2+1) \subseteq \mathbb{R}[X]$ is radical because $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$ is reduced. But $Z(I) = \emptyset$, so I is not of the form $\mathcal{I}(X)$ for any X (since we always have $X \subseteq Z(\mathcal{I}(X))$. However, the situation is better if k is algebraically closed as Hilbert's Nullstellensatz (proved by Hilbert in 1893) shows.

67. Theorem. (Hilbert's Nullstellensatz — Weak form) Let k be an algebraically closed field. Then M is a maximal ideal in the polynomial ring $k[X_1, \ldots, X_n]$ if and only if

$$M = (X_1 - a_1, \ldots, X_n - a_n)$$

for some $a_1, \ldots, a_n \in k$. Equivalently, the maps Z and $\mathcal{I}$ give a bijective correspondence

$$\{\text{points in } \mathbb{A}^n\} \underset{Z}{\overset{\mathcal{I}}{\rightleftarrows}} \{\text{maximal ideals in } A(\mathbb{A}^n)\}.$$

Moreoves, if I is any proper ideal in $k[X_1, \ldots, X_n]$ then $Z(I) \neq \emptyset$.

proof. Certainly $(X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal in $k[X_1, \ldots, X_n]$. Conversely, for any maximal ideal $\mathcal{M}$ in $k[X_1, \ldots, X_n]$, let $E = k[X_1, \ldots, X_n]/\mathcal{M}$. Then E is a field containing k that is finitely generated over k (by $\bar{X}_1, \ldots, \bar{X}_n$). By Noether's Normalization Lemma, we see that either E is algebraic over k or E is integral over a polynomial ring $k[y_1, \ldots, y_q]$. In the latter case, we obtain that $k[y_1, \ldots, y_q]$ is a field by Theorem 62 (1), and since a polynomial ring in one or more variables is never

a field we get a contradiction. It follows that E is algebraic over k. Because k is algebraically closed, $E=k$, i.e., $\overline{X}_i \in k$ for $1 \le i \le n$. Hence for $1 \le i \le n$, there is some $a_i \in k$ such that $X_i - a_i \in M$. This means that the maximal ideal $(X_1 - a_1, \ldots, X_n - a_n)$ is contained in M, so $M = (X_1 - a_1, \ldots, X_n - a_n)$. Finally, if I is any proper ideal in $k[X_1, \ldots, X_n]$, then I is contained in a maximal ideal $M = (X_1 - a_1, \ldots, X_n - a_n)$, and so $(a_1, \ldots, a_n) \in Z(I)$. □

68. Theorem. (Hilbert's Nullstellensatz) Let k be an algebraically closed field. Then for every ideal I of $k[X_1, \ldots, X_n]$, $\mathcal{I}(Z(I)) = \sqrt{I}$. Moreover, the maps Z and $\mathcal{I}$ define inverse bijections

$$\{\text{affine algebraic sets}\} \underset{Z}{\overset{\mathcal{I}}{\rightleftarrows}} \{\text{radical ideals}\}.$$

proof. Clearly $\sqrt{I} \subseteq \mathcal{I}(Z(I))$; it remains to prove the reverse inclusion. By Hilbert's Basis Theorem, $I = (f_1, \ldots, f_m)$ for some $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$. Let $g \in \mathcal{I}(Z(I))$. Introduce a new variable X_{n+1} and consider the ideal I' generated by $f_1, \ldots, f_m$ and $X_{n+1} g - 1$ in $k[X_1, \ldots, X_n, X_{n+1}]$. At any point of $\mathbb{A}^{n+1}$ where $f_1, \ldots, f_m$ vanish, the polynomial g also vanishes since $g \in \mathcal{I}(Z(I))$, so that $X_{n+1} g - 1$ is nonzero. Hence $Z(I') = \phi$ in $\mathbb{A}^{n+1}$. By the Weak Form of Nullstellensatz,

I' cannot be a proper ideal i.e., $1 \in I'$. Write

$$1 = a_1 f_1 + \cdots + a_m f_m + a_{m+1}(X_{n+1} g - 1)$$

for some $a_i \in k[X_1, \ldots, X_{n+1}]$. (etting $y = 1/X_{n+1}$ and multiplying by a high power of y in this equation shows that

$$y^N = c_1 f_1 + \cdots + c_m f_m + c_{m+1}(g - y)$$

for some $c_i \in k[X_1, \ldots, X_n, y]$. Substituting g for y in this polynomial equation shows that $g^N \in I$ (in $k[X_1, \ldots, X_n]$), i.e., $g \in \sqrt{I}$. Hence $\mathcal{I}(\mathcal{Z}(I)) \subset \sqrt{I}$, and so $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$, completing the proof. □