Then

$$R[s,t] = Rs_1t_1 + \cdots + Rs_it_j + \cdots + Rs_nt_m$$

is a ring containing $s \pm t$ and st that is also a finitely generated R-module. Hence $s \pm t$ and st are also integral over R, which proves (1) and also (2).

To prove (3), let $t \in T$. Since t is integral over S, it is the root of some monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in S[x]$. Since $a_i \in S$ is integral over R, each ring $R[a_i]$ is a finitely generated R-module and so the ring $R_1 = R[a_0, a_1, \ldots, a_{n-1}]$ is also a finitely generated R-module. Since the monic polynomial $p(x)$ has its coefficients in R_1, t is integral over R_1 and it follows that the ring $R_1[t] = R[a_0, a_1, \ldots, a_{n-1}, t]$ is a finitely generated R-module. By the proposition, this means that t is integral over R, which gives (3).

The second statement in Corollary 24 shows that taking the elements of S that are integral over R gives a (possibly larger) subring of S, and the last statement in the corollary shows that the process of taking the integral closure stops after one step:

Corollary 25. Let R be a subring of the commutative ring S with $1 \in R$. Then the integral closure of R in S is integrally closed in S.

Examples

(1) If R and S are fields then S is integral over R if and only if S is algebraic over R — if $s \in S$ is a root of the polynomial $p(x)$ with coefficients in R then it is a root of the monic polynomial obtained by dividing by the (nonzero) leading coefficient of $p(x)$.

(2) Suppose S is an integral extension of R and I is an ideal in S. Then S/I is an integral ring extension of $R/(R \cap I)$ (reducing the monic polynomial over R satisfied by $s \in S$ modulo I gives a monic polynomial satisfied by $\bar{s} \in S/I$ over $R/(R \cap I)$).

(3) If R is a U.F.D. then R is integrally closed, as follows. Suppose a/b is an element in the field of fractions of R (with $b \neq 0$ and a and b having no common factors) and satisfies $(a/b)^n + r_{n-1}(a/b)^{n-1} + \cdots + r_1(a/b) + r_0 = 0$ with $r_0, \ldots, r_{n-1} \in R$. Then

$$a^n = b(-r_{n-1}a^{n-1} - \cdots - r_1ab^{n-2} - r_0b^{n-1})$$

shows that any irreducible element dividing b divides a^n, hence divides a. Since a/b is in lowest terms, this shows that b must be a unit, i.e., $a/b \in R$.

(4) The polynomial ring $k[x, y]$ over the field k is integrally closed in its fraction field $k(x, y)$ by example (3) above. The ideal $(x^2 - y^3)$ is prime (cf. Exercise 14, Section 9.1), so the quotient ring $R = k[x, y]/(x^2 - y^3) = k[\bar{x}, \bar{y}]$ is an integral domain. This domain is not integrally closed, however, since $\bar{x}/\bar{y}$ is an element of the fraction field of R that is integral over R (since $(\bar{x}/\bar{y})^3 - \bar{x} = 0$), but is not an element of R. In particular, R is not a U.F.D. by the previous example.

We next consider the behavior of ideals in integral ring extensions.

Definition. Let $\varphi : R \to S$ be a homomorphism of commutative rings.

(a) If I is an ideal in R then the *extension* of I to S is the ideal $\varphi(I)S$ of S generated by the image of I.

(b) If J is an ideal of S, then the *contraction* in R of J is the ideal $\varphi^{-1}(J)$.

In the special case where R is a subring of S and φ is the natural injection, the extension of $I \subseteq R$ is the ideal IS in S and the contraction of $J \subseteq S$ is the ideal $J \cap R$ of R.

It is immediate from the definition that

(1) $I \subseteq IS \cap R$, more generally, I is contained in the contraction of its extension to S, and
(2) $(J \cap R)\, S \subseteq J$, more generally, J contains the extension of its contraction in R.

In general equality need not hold in either situation (cf. the exercises).

If Q is a prime ideal in S, then its contraction is prime in R (although the contraction of a maximal ideal need not be maximal). On the other hand, if P is a prime ideal in R, its extension need not be prime (or even proper) in S; moreover, it is not generally true that P is the contraction of a prime ideal of S (cf. the exercises). For integral ring extensions, however, the situation is more controlled:

Theorem 26. Let R be a subring of the commutative ring S with $1 \in R$ and suppose that S 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) Let P be a prime ideal in R. Then there is a prime ideal Q in S with $P = Q \cap R$. Moreover, P is maximal if and only if Q is maximal.
(3) *(The Going-up Theorem)* Let $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$ be a chain of prime ideals in R and suppose there are prime ideals $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m$ of S with $P_i = Q_i \cap R$, $1 \leq i \leq m$ and $m < n$. Then the ascending chain of ideals can be completed: there are prime ideals $Q_{m+1} \subseteq \cdots \subseteq Q_n$ in S such that $P_i = Q_i \cap R$ for all i.
(4) *(The Going-down Theorem)* Assume that S is an integral domain and R is integrally closed in S. Let $P_1 \supseteq P_2 \supseteq \cdots \supseteq P_n$ be a chain of prime ideals in R and suppose there are prime ideals $Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_m$ of S with $P_i = Q_i \cap R$, $1 \leq i \leq m$ and $m < n$. Then the descending chain of ideals can be completed: there are prime ideals $Q_{m+1} \supseteq \cdots \supseteq Q_n$ in S such that $P_i = Q_i \cap R$ for all i.

Proof: To prove (1) assume first that R is a field and let s be a nonzero element of S. Then s is integral over R, so

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

for some $a_0, a_1, \ldots, a_{n-1}$ in R. Since S is an integral domain, we may assume $a_0 \neq 0$ (otherwise cancel factors of s). Then

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

and since $(-1/a_0) \in R$, this shows that $(-1/a_0)(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1)$ is an inverse for s in S, so S is a field. Conversely, suppose S is a field and r is a nonzero element of R. Since $r^{-1} \in S$ is integral over R we have

$$r^{-m} + a_{m-1}r^{-m+1} + \cdots + a_1 r^{-1} + a_0 = 0$$

for some $a_0, \dots, a_{m-1} \in R$. Then $r^{-1} = -(a_{m-1} + \cdots + a_1 r^{m-2} + a_0 r^{m-1}) \in R$, so R is a field.

The proof of the first statement in (2) is given in Corollary 50. For the second statement, observe that the integral domain S/Q is an integral extension of R/P (Example 2 following Corollary 25). By (1), S/Q is a field if and only if R/P is a field, i.e., Q is maximal if and only if P is maximal.

To prove (3), it suffices by induction to prove that if $P_1 \subseteq P_2$ and Q_1 is a prime of S with $Q_1 \cap R = P_1$ then there is a prime Q_2 of S with $Q_1 \subseteq Q_2$ and $Q_2 \cap R = P_2$. Since $\overline{S} = S/Q_1$ is an integral extension of $\overline{R} = R/P_1$, the first part of (2) shows that there exists a prime $\overline{Q_2}$ of $\overline{S}$ with $\overline{Q_2} \cap \overline{R} = P_2/P_1$. Then the preimage Q_2 of $\overline{Q_2}$ in S is a prime ideal containing Q_1 with $Q_2 \cap R = P_2$.

The proof of (4) is outlined in Exercise 24 in Section 4.

Corollary 27. Suppose R is a subring of the ring S with $1 \in R$ and assume S is integral and finitely generated (as a ring) over R. If P is a maximal ideal in R then there is a nonzero and finite number of maximal ideals Q of S with $Q \cap R = P$.

Proof: There exists at least one maximal ideal Q lying over P by (2) of the theorem, so we must see why there are only finitely many such maximal ideals in S. If Q is a maximal ideal of S with $Q \cap R = P$ then S/Q is a field containing the field R/P. To prove that there are only finitely many possible Q it suffices to prove that there are only finitely many homomorphisms from S to a field containing R/P that extend the homomorphism from R to R/P. Let $S = R[s_1, \dots, s_n]$, where the elements s_i are integral over R by assumption, and let $p_i(x)$ be a monic polynomial with coefficients in R satisfied by s_i. If Q is a maximal ideal of S then $S/Q = (R/P)[\bar{s}_1, \dots, \bar{s}_n]$ is the field extension of the field R/P with generators $\bar{s}_1, \dots, \bar{s}_n$. The element $\bar{s}_i$ is a root of the monic polynomial $\bar{p}_i(x)$ with coefficients in R/P obtained by reducing the coefficients of $p_i(x)$ mod P. There are only a finite number of possible roots of this monic polynomial (in a fixed algebraic closure of R/P), and so only finitely many possible field extensions of the form $(R/P)[\bar{s}_1, \dots, \bar{s}_n]$, which proves the corollary.

Algebraic Integers

We can use the concept of an integral ring extension to define the "integers" in extension fields of the rational numbers $\mathbb{Q}$:

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 $\mathbb{Z}$, i.e., if α is the root of some monic polynomial with coefficients in $\mathbb{Z}$.

(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 $\mathbb{Q}$. Examples of algebraic integers include $\sqrt{2}$, $\sqrt{-1}$, $\sqrt[3]{5}$, etc. since these elements are certainly roots of monic polynomials with coefficients in $\mathbb{Z}$. The definition of an algebraic integer α is that α be a root